VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

# BAKALÁŘSKÁ PRÁCE

Brno, 2019 Tomáš Krejča


# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

## ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS


# LABORATORNÍ ÚLOHA ELEKTRONICKÁ KONTROLA VSTUPU
LABORATORY EXERCISE ELECTRONIC ACCESS CONTROL

**BAKALÁŘSKÁ PRÁCE**
BACHELOR'S THESIS


**AUTOR PRÁCE** — **Tomáš Krejča**
AUTHOR

**VEDOUCÍ PRÁCE** — **doc. Ing. Karel Burda, CSc.**
SUPERVISOR



**BRNO 2019**

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

# Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

***Student:*** Tomáš Krejča ***ID:*** 195674
***Ročník:*** 3 ***Akademický rok:*** 2018/19

**NÁZEV TÉMATU:**

## Laboratorní úloha Elektronická kontrola vstupu

**POKYNY PRO VYPRACOVÁNÍ:**

Nastudujte a popište problematiku systémů elektronické kontroly vstupu (EKV). Na základě dodaných komponent navrhněte a zrealizujte výukový systém EKV. Pro vytvořený systém navrhněte a ověřte laboratorní úlohu a zpracujte pro ni dokumentaci jak pro studenty, tak i vyučujícího. Rovněž vytvořte technickou dokumentaci systému EKV.

**DOPORUČENÁ LITERATURA:**

[1] Burda K.: Základy elektronických zabezpečovacích systémů. CERM, Brno 2018.

[2] Příručka k uvedení systému NetAXS-123 do provozu. Honeywell, Brno 2010.

***Termín zadání:*** 1.2.2019 ***Termín odevzdání:*** 27.5.2019

***Vedoucí práce:*** doc. Ing. Karel Burda, CSc.
***Konzultant:***

**prof. Ing. Jiří Mišurec, CSc.**
*předseda oborové rady*

## ABSTRAKT

Tato bakalářská práce práce je rozdělena na teoretickou a praktickou část, v teoretické části zabývá popisem systémů Elektronické kontroly vstupu EKV, jsou popsány výhody nasazování těchto systémů, jejich architektura, možnosti budoucího vývoje v rámci sítě IP a napájení pomocí technologie Power over Ethernet. Blíže seznamuje taky s využívaným komunikačním rozhraním Wiegand. V textu jsou popsány jednotlivé metody autentizace a identifikační technologie, největší prostor je věnován radiofrekvenčním RFID kartám a dnes již méně využívaných magnetických a Wiegandových karet, nastíněna je také technologie NFC. Z biometrických technologí je popsána optická metoda snímání otisků prstů.

V praktické části se práce věnuje návrhu laboratorní úlohy EKV na základě dodaných komponent, které jsou v textu popsány. Je zpracováno schéma zapojení systému, popsání jeho možností. Na tomto základu je sepsán návod Laboratorní úlohy elektronické kontroly vstupu pro studenty a text doplňujících informací pro vyučující. Sestavení a zapojení systému je rozebráno v kapitole Technická dokumentace.



## KLÍČOVÁ SLOVA

Elektronická kontrola vstupu, Kontrolér, Morphomanager, Terminál, Wiegand, WIN-PAK.



## ABSTRAKT

This bachelor thesis is divided to theoretical and practical part, in theoretical part deals with description Access control systems ACS. The benefits of deploying systems are discussed, your architecture, opportunities for future development in IP sites and power over technology Power over Ethernet. Introduces the use of the interface Wiegand. In text are described individual authentication and identification technology. The largest space is devoted to radiofrequency technology and now unused magnetic and Wiegand cards. Outlined is NFC technology. From biometric technology is described optical method fingerprinting.

In the practical part, the thesis deals with the design of laboratory exercise. The supplied components are described in the text. The involvement and description of the options is worked out. The thesis contains the text of the laboratory exercise of electronic access control for students and additional text for teachers. Assembly and connection of the system is in the chapter Technical documentation.



## KLÍČOVÁ SLOVA

Access control system, Controller, Morphomanager, Terminal, Wiegand, WIN-PAK.

KREJČA, Tomáš. *Laboratorní úloha Elektronická kontrola vstupu*. Brno, Rok, 50 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: doc. Ing. Karel Burda, CSc.

# PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Laboratorní úloha Elektronická kontrola vstupu“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ..... .....

podpis autora

# PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu doc.Ing. Karlu Burdovi, CSc. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.


Brno ..... .....

podpis autora

# Obsah

# Seznam obrázků

# 1 Elektronická kontrola vstupu

## 1.1 Důvody nasazení EKV

Systémy EKV nasazujeme zejména z důvodu omezení vstupu neoprávněných osob do vyhrazených prostor, možnosti časově tento přístup omezit (to lze využít pro externí subjekty vstupující do objektu nebo návštěvy) a sledování času příchodů a odchodu osob, což je možné využít pro následné zpracování docházky zaměstnanců.

Systémy EKV může pružně spravovat autorita. Nehrozí ztráta klíčů uživately, případně zneužití klíčů pro neoprávněný vstup do objektu třetí osobou. V případě ztráty identifikačního média u systémů EKV lze oprávnění ke vstupu do objektu odebrat autoritou. Další výhodou je to, že není třeba vyrábět přesné kopie klíčů nebo zámkových systémů při rozšiřování objektu nebo navyšování počtu zaměstnanců. Snižuje se nebezpečí neuzamknutí vstupu osobou s oprávněním vstupu do vyhrazeného prostoru, tj. osoba nemusí myslet na uzamčení dveří klíčem při odchodu.

Systém EKV lze využít také jako platební a odbavovací systém. Můžeme umožnit prodej vstupenek na základě přiděleného identifikačního čipu a řídit pohyb osob v areálu nebo parkovištích. Využití například pro aquaparky, sportovní a relaxační zařízení, kulturní akce, koncerty a další.

Úsporná opratření v budovách. Možnost využití v hotelech, kdy po odchodu ubytovaného z pokoje dojde k automatickému vypnutí elektřiny v pokoji, případně odpojení některých z okruhů - typicky světelné obvody.

## 1.2 Struktura systémů EKV

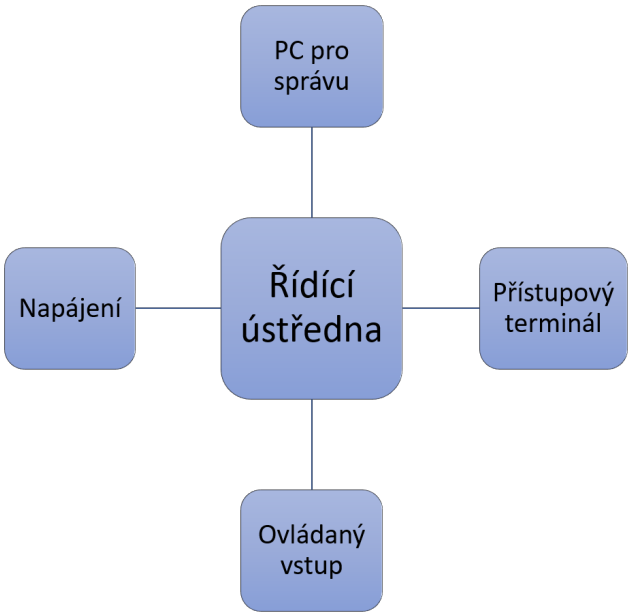
Systémy elektronické kontroly vstupu jsou architekturou podobné jiným systémům rodiny zabezpečovacích systémů, kterými jsou:

- Poplachové a tísňové zabezpečovací systémy PTZS (dříve elektronická zabezpečovací signalizace EZS).
- Elektrická požární signalizace EPS.
- Dohledové video systémy DVS (dříve uzavřený televizní okruh či Closed Circuit Television CCTV).

U těchto systémů je jádrem speciální hardwarové zařízení, běžně pojmenovávané jako ústředna, řídicí ústředna či řidicí kontrolér, které komunikuje s připojenými periferiemi pomocí komunikačního rozhraní.

Systémy EKV se musejí skládat minimálně z těchto konponent:

1. Přístupová ústředna či řídicí ústředna.
2. Přístupový terminál.
3. Ovládaný vstup.
4. Komunikační rozhraní.
5. Napájení.




Obr. 1.1: Blokové schema systému EKV.

## 1.3 Možnosti kombinace EKV s dalšími systémy

1. Kombinace systému EKV s docházkovými systémy:
   Kombinace ke které systém EKV vybízí a je standartním doplňkem v organizacích. Díky této kombinaci může zaměstnavatel sledovat nejen příchod/odchod zaměstnance, ale i odchod na přestávky; odchod k lékaři; aktuální čerpání dovolené; odchod ze zaměstnání z důvodu úrazu a jiné. Systém může být zpřístupněn i samotným zaměstnancům, kteří mohou sledovat vlastní strávený čas v zaměstnání nebo ověřovat zdali je jiný zaměstnanec přítomen. To je výhodné pro ověření toho, jestli se kolega nachází/nenachází v práci a je možné ho kontaktovat či nikoliv.

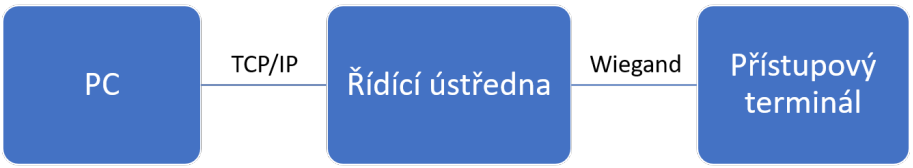
2. Kombinace systému EKV se systémem výdeje stravy:
   Pomocí jednoho identifikačního média lze zpřístupnit i jiné systémy, může jít například o evidenci výdeje stravy, pracovních pomůcek a další. Nemusíme tak archivovat několik evidencí pro jednoho zaměstnance, přijímaná data můžeme zpracovávat ve vhodných databázích a vést jen jednu evidenci pro každého zaměstnance při evidování více služeb.

3. Kombinace systému EKV se systémy PTZS:
   Nabízí se taková konfigurace, kdy při prvním vstupu autorizovanou osobou do objektu je automaticky deaktivován celý či část PTZS.

4. Kombinace systému EKV se systémem EPS:
   Použití takové kombinace je oceněno při rizikových situacích. Příkladem je situace, kdy ústředna EPS vyhlásí poplach v objektu. V případě absence propojení systémů dojde k bezpečnostnímu problému, kdy by systém EKV mohl působit problémy nejen při opouštění areálu personálem - zejména pokud jsou instalovány čtečky na obou stranách vstupu, ale i při možném zásahu hasičů. Aby jsme zamezili těmto jevům, propojujeme systémy tak, aby při ohlášení požáru systémem EPS došlo automaticky k odemčení všech vstupů ovládaných systémem EKV.

## 1.4 Komunikace v systémech kontroly vstupu

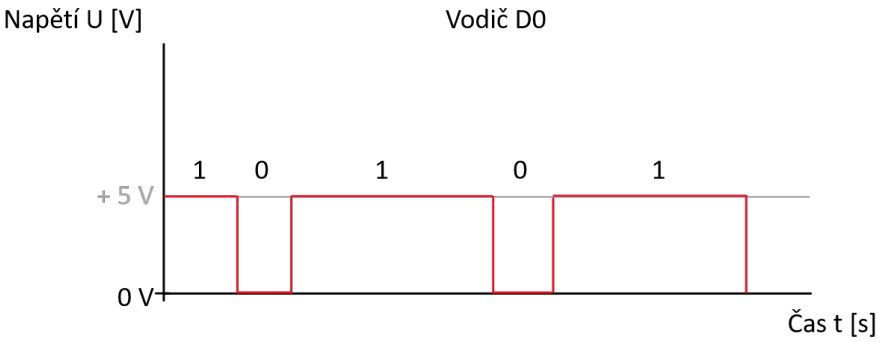
Současné systémy nabízejí několik komunikačních rozhraní pro vzájemnou komunikaci PC s ústřednou, zejména kvůli udržování zpětné kompatibility se staršími zařízeními. V budoucnu se počítá s komunikací zejména pomocí UTP kabelů. Pro komunikaci ústředny s terminály se z historických důvodu využívá nejčastěji rozhraní Wiegand (lze využít i RS 485 nebo RS 232).




Obr. 1.2: Druhy komunikace v systémech elektronické kontroly vstupu.

### 1.4.1 Wiegandovo rozhraní

Wiegandovo rozhraní či Wiegandova sběrnice označuje jednosměrný komunikační kanál využívaný pro komunikaci mezi ústřednou a přístupovým terminálem, přičemž maximální vzdálenost mezi zařízeními by neměla překročit 150 metrů. Systém využívá k signalizaci napětí +5 V na dvou vodičích označovaných D0 a D1. Pomocí odpínání napětí signalizujeme logickou 0 nebo 1, je-li odpojeno napětí na vodiči D0 je vyslána logická 0, přičemž na vodiči D1 zůstává plné napětí 5 V. Je-li odpojeno napětí na vodiči D1, signalizujeme logickou 1. Aby došlo ke správnému rozpoznání logické hodnoty obvody, je pro pokles napětí vyhrazen čas 50 µs a odstup mezi poklesy 1 ms (hodnoty se můžou lišit dle specifikace výrobce).




Obr. 1.3: Určení logických hodnot na datovém vodiči D0 Wiegandovy sběrnice.

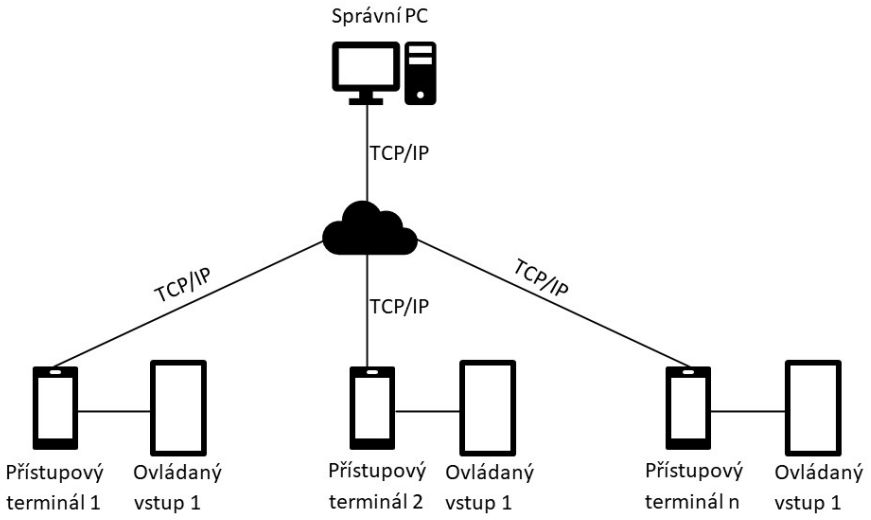
Sběrnice dále obsahuje vodič GND pro uzemnění a napájecí vodič pro napájení terminálu. Další vodiče mohou být dododávány výrobcem (např. LED signalizace nebo bzučák). V praxi jsou nejčastější 5 a 6 vodičové systémy.

## 1.5 Vývojové trendy

Budoucí vývoj systémů elektronické kontroly vstupu se dle mého názoru bude ubírat postupným začleňováním do sítí komunikujících na protokolu TCP/IP. Již v současné době je standard, že kontrolér v síti IP komunikuje s obslužným programem, terminály pak s kontrolérem komunikují pomocí Wiegandova protokolu. Výrobci ale dnes nabízejí terminály, které jsou přímo připojitelné do IP sítě, viz. kapitola 1.5.1. Stále častější je také napájení pomocí UTP kabelů, označované jako PoE (Power over Ethernet) napájení. Více o napájení pomocí PoE v kapitole 1.5.2.

### 1.5.1 Začlenění systémů kontroly vstupu do datových sítí

Reálným vývojem je začlení systémů kontroly vstupu do datových sítí komunikujících pomocí protokolu TCP/IP. V tomto případě by z celého systému odpadla funkce kontroléru a jednotlivé přístupové terminály by se chovaly jako koncová zařízení sítě. Takovým způsobem funguje většina biometrických terminálů, protože biometrické metody autentizace jsou vzájemně odlišné a dané metodě musí být uzpůsobena hardware a firware zařízení. Z tohoto důvodu autentizaci provádí terminál, který se tak zároveň chová jako kontrolér.




Obr. 1.4: Přístupové terminály v rámci datové sítě.

Výhodami systému EKV v rámci datové sítě je jednotká kabeláž UTP s koncovkami RJ-45 v celém objektu nebo možnost instalovat terminál kdekoliv v dosahu datové sítě, nemusíme se tak vázat na vzdálenost ústředny. Nevýhodami vyšší nároky na zabezpečení, jednak samotné čtečky v rámci datové sítě - přístupovým loginem a heslem. Samotná komunikace v rámci datové sítě musí podléhat zabezpečení a kontrole, např. proti podvržení falešného paketu potvrzující správnou identitu osoby. Další nevýhodou je nutnost použití převodníku Ethernet a tedy vyšší ceny IP terminálů oproti klasickým komunikujících pomocí sběrnic Wiegand, případně RS 485 nebo RS 232.

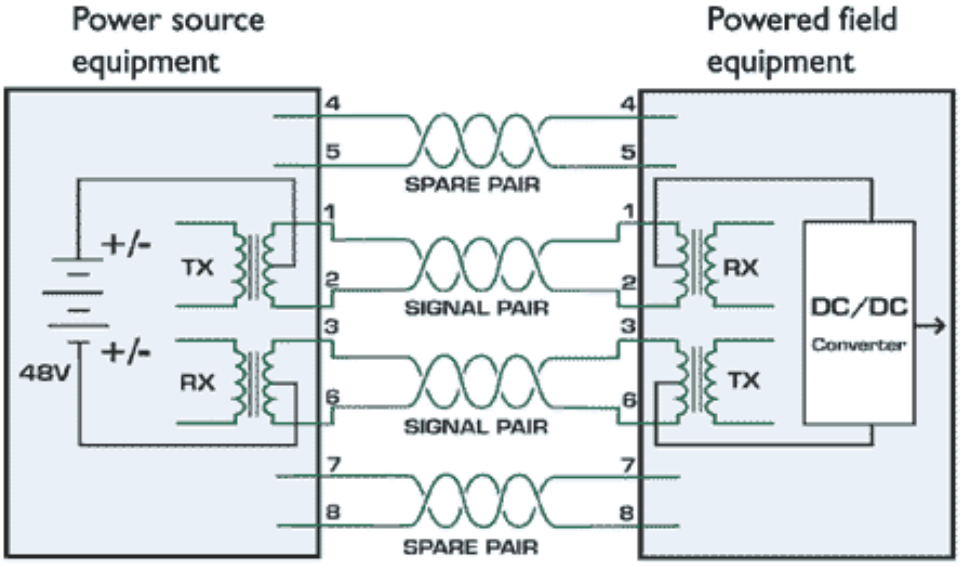
### 1.5.2 Power over Ethernet

Jedná se o technologii, která umožňuje napájet zařízení pomocí ethernetových kabelů při zachování datového připojení. Rozlišujeme 2 druhy technologie PoE:

- Pasivní PoE (standard IEEE 802.3at).
- Aktivní PoE (standard 802.3af).

Pasivní PoE definováno standardem 802.3at, kde je napájení vedeno přes nevyužité vodiče v ethernet kabelu. Kvůli nutnosti samostatných vodičů, nevyužívaných pro přenos dat, není možné použití u gigabitových přenosů. Gigabitový ethernet využívá pro přenos dat všechny 4 páry vodičů. 10 a 100 Mbit ethernet využívá pro přenos dat 2 páry a další 2 páry jsou nevyužité a je na nich možné využít pasivní PoE, 2 vodiče pak slouží jako napájecí a 2 jako zem. Pasivní PoE nevyjednává potřebnou velikost napětí.

Aktivní PoE je definováno standardem 802.3af, zařízení si vyjednají potřebné napětí, čímž je sníženo nebezpečí poškození zařízení vysokým napětím. Narozdíl od pasivní technologie PoE se využívá tzv. Fantomové napětí, které vedeme přímo po datových vodičích. Z tohoto důvodu je technologie využitelná i u gigabitových ethernetových kabelů.




Obr. 1.5: Princip PoE dle standardu IEEE 802.3af. Převzato z [8].

Proces vyjednávání potřebného napětí probíhá ve 3 krocích:

1. Detekce zařízení komptabilního se standardem IEEE 802.3af.
2. Určení výkonové třídy napájeného zařízení.
3. Napájené zařízení zahájí odběr potřebný pro svou činnost.

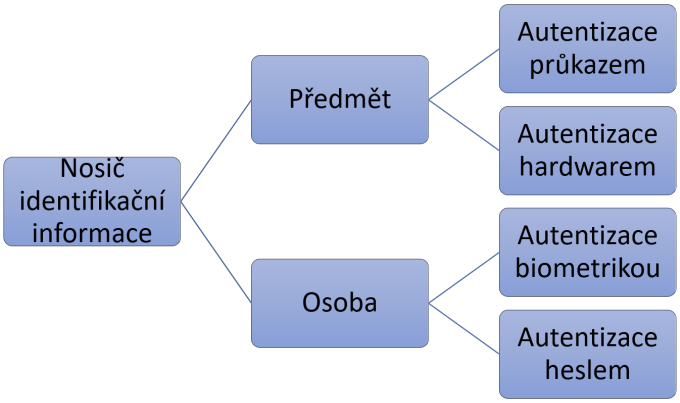
Existuje 5 výkonových tříd, přičemž v současné době jsou používány 4 a 5. (respektivě 4.) je vyhrazena pro budoucí využití a 1. (respektivě 0.) třída je využívána jen v případě, že nedojde ke správné identifikaci napájeného zařízení.

| Třída | Proud I | Max. příkon NZ | Max. výkon ZN |
|---|---|---|---|
| 0 | 0 - 4 mA | 12,95 W | 15,4 W |
| 1 | 9 - 12 mA | 3,84 W | 4 W |
| 2 | 17 - 20 mA | 6,49 W | 7 W |
| 3 | 26 - 30 mA | 12,95 W | 15,4 W |
| 4 | 36 - 40 mA | 12,95 W | 15,4 W |

Obr. 1.6: Výkonové třídy PoE dle standardu IEEE 802.3af. Převzato z [8].

# 2 Metody autentizace

Hlavním úkolem systémů elektronické kontroly vstupu je ověřovat identititu a autentizovat osobu na základě autorizace přidělenou autoritou. Toto ověřování probíhá pomocí přístupových terminálů, na základě tohoto ověření je systémem řízen vstup. Existuje celá řada metod identifikace osoby, které od autorizované osoby požadují různé vlastnosti. Použité metodě musí být přizpůsobeno hardwarové řešení přístupové čtečky. Celkově můžeme druhy ověřování identity dělit následovně:




Obr. 2.1: Rozdělení autentizačních metod.

Přičemž autentizace průkazem se v dnešních systémech elektronické kontroly vstupu nevyužívá z důvodu časové náročnosti na ověření identity, které musí provádět osoba. Zařízení pro kontrolu průkazu i samotné průkazy navíc bývají drahé.

## 2.1 Autentizace heslem

Metoda autentizace uživatele heslem zakládá na tom, že uživatel má znalost unikátního kódu, který je znám nejlépe jen jemu samotnému. Uživatel provádí autentizaci tím způsobem, že jemu známou posloupnost znaků musí ve správném pořadí zadat do přístupového terminálu. Výhoda metody spočívá v tom, že uživatel nemusí mít fyzický identifikační předmět, snižují se tak nejen pořizovací a provozní náklady systému EKV. V dnešní době se od této metody identifikace v systémech Elektronické kontroly vstupu upouští, případně se kombinuje s jinými metodami.

V informačních technologích se ovšem jedná stále o nejpoužívanější způsob ověřování identitity uživatele. Běžně je tento typ identifikace využívám při řízení přístupu do stolních počítačů, notebooků, mobilních telefonů aj. Mimo jiné jej využívá řada chráněných služeb do kterých je přistupováno pomocí internetu, např. internetové bankovnictví, vertifikace plateb přes internet a další.

## 2.2 Autentizace hardwarem

Tato metoda autentizace, narozdíl od předchozích dvou, zakládá na tom, že osoba při sobě musí mít určitý předmět. Tento předmět v sobě má zapsanou jedinečnou informaci, která identifikuje jeho vlastníka. Existuje více hardwarových řešení identifikačních předmětů (médií):

- Karty s magnetickým proužkem,
- Wiegandovy karty,
- optické systémy,
- radiofrekvenční (RFID) karty,
- mikroprocesorové karty,
- chytré mobilní telefony (smartphone).

Principy jednotlivých hardwarových řešení budou popsány v kapitole: Identifikační technologie.

## 2.3 Autentizace biometrikou

Autentizace osoby biometrikou využívá jedinečné tělesné vlastnosti každé osoby. Narozdíl od předchozích metod není nutné si pamatovat heslo nebo nosit identifikační předmět, identifikačním předmětem je samotná osoba podrobovaná autentizaci.

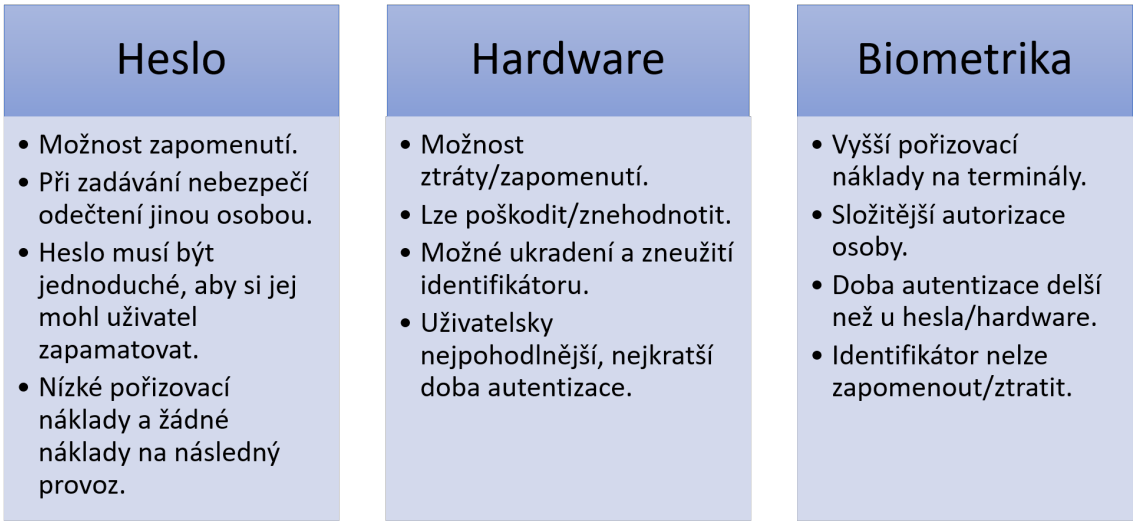
Každý uživatel je nejprve podroben procesu, kdy se snažíme získat co nejpřesnější a nejkvalitnější referenční vzor vybrané biometrické veličiny. Tato sejmutá biometrika osoby je následně zapsána do paměti zařízení. Při každé žádosti o přístup do kontrolované oblasti žadatel o přístup předkládá jako autentizační předmět vlastní biometrickou veličinu, tato biometrika je porovnávána s referenční hodnotou, která se musí aktuálně předložené maximálně blížit.

V závislosti na druhu biometriky, kterou u dané osoby podrobujeme kontrole, rozlišujeme následující biometrické technologie:

- Geometrie ruky,
- duhovka oka,
- sítnice oka,
- otisk prstu,
- akustická charakteristika hlasu,
- DNA.

Dalšími možnými, ale méně používanými biometrikami jsou např.: Geometrie tváře, způsob pohybu očí, struktura žil na zápěstí, behaviometrika, psaní na klávesnici, dynamika chůze, identifikace dle pachu, biometrie ušního boltce, spektroskopie kůže, bioelektrické pole, biodynamický popis osoby, biometrické vlastnosti zubů.

## 2.4 Porovnání jednotlivých metod

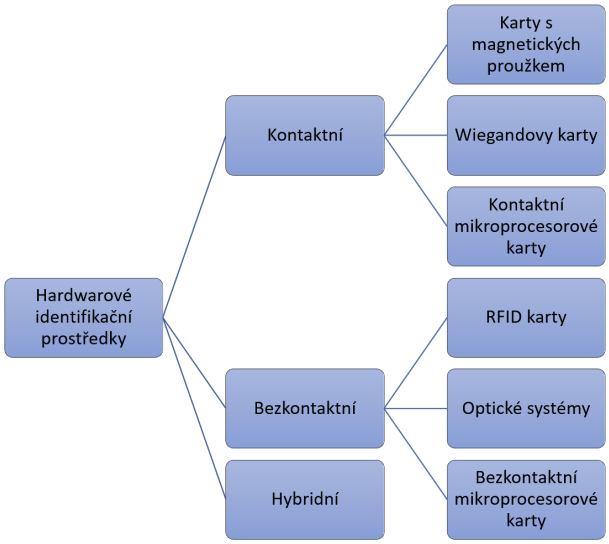



Obr. 2.2: Porovnání jednotlivých metod, jejich výhody a nevýhody.

# 3 Identifikační technologie

V této kapitole budou popsány jednotlivé hardwarové a biometrické identifikační technologie. Popsány budou karty s magnetickým proužkem a Wiegandovy karty, tyto technologie se dnes nenasazují, ale historicky právě tyto technologie pomohly k rozšíření systémů elektronické kontroly vstupu. Dále v současné době využívaná radiofrekvenční technologie, která je použita v praktické části semestrální práce a nastíněna technologie NFC, která má budoucí využití hlavně při nasazení autentizace chytrými telefony.

Z biometrických metod se kapitola věnuje snímání otisků prstů pomocí optických senzorů, tato metoda je využita v praktické části bakalářské práce.



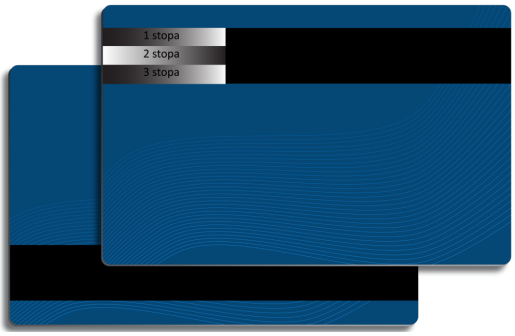

Obr. 3.1: Dělení identifikačního hardwaru.

Pozn. v rozdělení jsou také zmíněny optické systémy, kterými se myslí identifikace pomocí čárových (bar) kódů, tato identifikace je typická spíše pro zboží, je ale možné ji nasadit i k identifikaci osoby jako doplněk některé jiné identifikační technologie.

## 3.1 Karty s magnetickým proužkem

Základem karty je magnatický proužek složený s malých kovových částaček, které je možno zmagnetizovat. Po zmagnetizování silným magnetickým polem se na povrchu vytvoří malé permanentní magnety, pomocí kterých definujeme data zapsaná na kartě. Tyto data jsou na kartě zapsána ve 3 stopách, kde 2 stopy jsou určeny pro čtení a 1 stopa pro zápis.

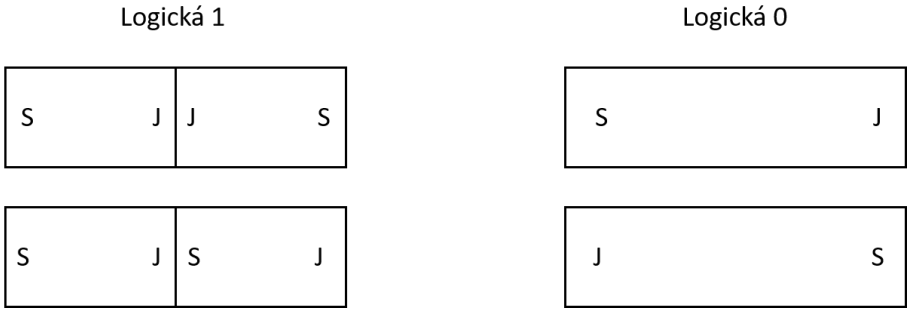
- 1. stopa (IATA) obsahující jen alfanumerické znaky,
- 2.stopa (ABA) pro numerické znaky a




Obr. 3.2: Příklad karty s magnetickým proužkem. Převzato z [4].

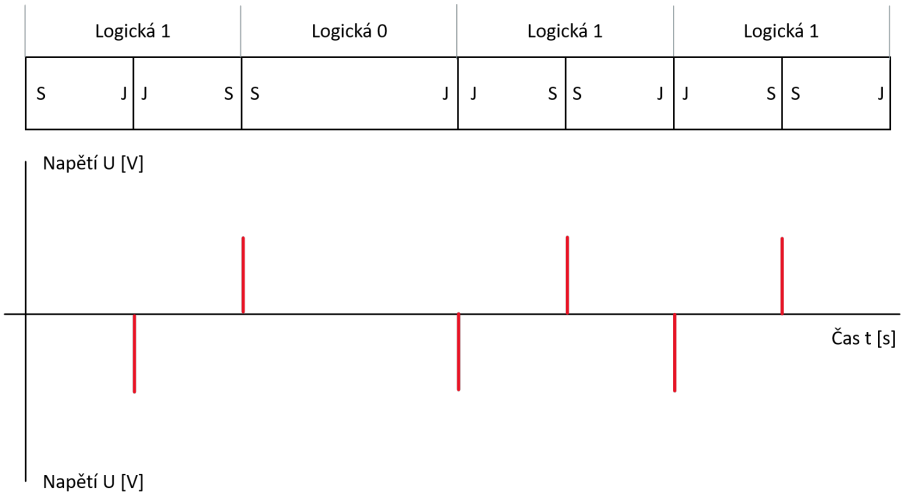
- 3. stopa (THRIFT) pro numerické znaky.

Informace na kartě je zapsána pomocí logických hodnot, kdy log. 0 představuje jeden magnet a log. 1 dvojici magnetů, které jsou vzájemně opačně orientované. Z toho vyplývá, že data na kartu musí být zapisována s takovou přesností, aby nedocházelo k ovlivňování těch bitů, které nejsou aktuálně přepisovány.




Obr. 3.3: Princip zápisu logických hodnot na magnetický proužek.

Čtení hodnot z karty probíhá pomocí protahovacím čtecím zařízením. Při posunu magnetického proužku ve štěrbině vzniká v důsledku pohybu změna magnetického pole, čímž se indukuje napětí, označované jako elektromotorické napětí. Velikost tohoto napětí, je závislá na velikosti změny magnetického pole a rychlosti této změny. Elektromotorické napětí je v závisloti na orientaci magnetů indikováno čtečím zařízením. Možný průběh napětí lze vidět na následujícím obrázku.




Obr. 3.4: Princip čtení logických hodnot z magnetického proužku.

## 3.2 Wiegandovy karty

### 3.2.1 Wiegandův jev

Wiegandův jev popisuje chování magnetického pole ve speciálně konstruovaném vodiči protékaného proudem. Tomuto drátu říkáme Wiegandův drát, jedná se o slitinu kobaltu, železa a vanadu. Drát je zpracován tak, že tvoří tvrdý vnější plášť kolem měkkého vnitřního jádra. Působením vnějšího magnetického pole lze jeddnoduše magnetizovat vnější plášť, který odolaváná demagnetizaci při odložení vnějšího magnetického pole. Vnitří jádro je zmagnetizováno až po plném zmagnetizování vnějšího pláště. Při zániku mag. pole se jádro vrátí ke své magnetické orientaci před zmagnetováním. Toto „přepínání“ indukuje napětí na cívce, přičemž 1 impulz (změna orientace) má standartní délku 10µs.

## 3.3 Radiofrekvenční (RFID) karty

Radiofrekvenční karty komunikují s přístupovým terminálem pomocí elektromagnetických vln vysílaných na rádiové frekvenci. Podle kmitočtového pásma ve kterém komunikace probíhá, rozlišujeme 4 základní druhy radiofrekvenčních systémů:

### 3.3.1 Radiofrekvenční systémy

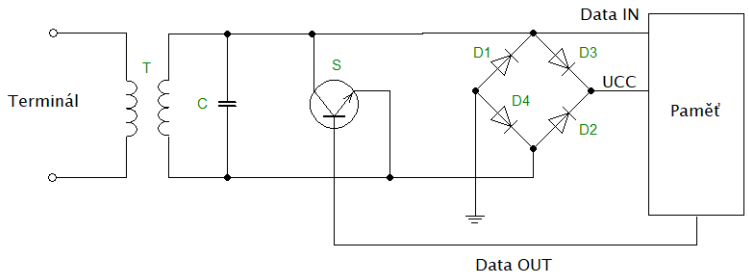
1. Nízkofrekvenční systémy LF (Low frequency) pracující s kmitočty 125 kHz nebo 135 kHz. Nevýhodou těchto systémů je dosah okolo 0,2 metru, maximálně 0,5 metru. Využití pro přístupové systémy - RFID systémy nebo identifikaci zvířat.
2. Vysokofrekvenční systémy HF (High frequency) pracují na kmitočtu 13,56 MHz, oproti LF systémů mají větší dosah i vyšší přesovou rychlost. Využití pro přístupové systémy - bezkontaktní mikroprocesorové karty; bezkontaktní placení; označování zavazadel při přepravě nebo identifikace zboží ve skladech.
3. UHF (Ultra high frequency) systémy pracující v kmitočtovém pásmu 860 MHz až 930 MHz. Přesné vymezení kmitočtového pásma je určeno jednotlivými zeměmi - což je částečnou nevýhodou těchto systémů. V EU je standartizováno pásmo 865 až 868 MHz. Dosah tohoto systému je okolo 6 metrů. Využití pro elektronické mýtné; současná identifikace více zabalených produktů.
4. Mikrovlné systémy pracující na kmitočtech 2,45 GHz nebo 5,8 GHz. Dosah systému je maximálně 2 metry. Využití pro elektronické mýtné; identifikace zavazedel v letecké přepravě nebo bezdrátový záznam a přenos dat v reálném čase.

### 3.3.2 Aktivní a pasivní RFID karty

RFID karty můžeme dělit podle druhu zdroje napájení karty na aktivní a pasivní.

1. Aktivní RFID karty využívají pro napájení svých obvodů interního napájecího zdroje. Toto řešení umožňuje kartám komunikovat na větší vzdálenosti, jedná se ale o dražší technologii oproti pasivním kartám.

2. Pasivní RFID karty využívájí energie elektromagnetických vln generovaných terminálem. Terminál vysílá rádiové vlny nepřetržitě, nejčastěji na frekvenci 125 kHz. Princip přenosu energie je ve vytvoření induktivní vazby mezi kartou a terminálem, která vznikne pri dostatečném vzdálenosti obou prvků. Přijímanou energií je nabit kondenzátor C, uložená energie slouží pro napájení paměťových a vysílacích obvodů karty. Paměť odesílá odpověď terminálu pomocí přepínače realizovaného tranzistorem, kdy jsou vysílány logické hodnoty 1 a 0. Podle toho, zda se vysílá logická 1 nebo 0 se zatěžuje nebo odlehčuje indukční pole cívky, čímž vznikne tzv. zátěžová modulace, tj. nepřímá amplitudově/fázová modulace.




Obr. 3.5: Elektrické schema pasivní RFID karty. Převzato z [5].

## 3.4 Identifikace smartphonem

### 3.4.1 Technologie NFC

Technologie NFC (Near field communication) označuje bezdrátový přenos dat uskutečňovaný pomocí radiofrekvenčního systému (RFID). Podobně jako RFID karty je můžeme dělit dle zdroje elektrické energie na aktivní a pasivní.

- Pasivní NFC zařízení zahrnují tagy a malé vysílače bez vlastního zdroje energie. V praxi se s pasivními NFC setkáváme ve formě značek na stěnách nebo jako reklamní sdělení, kde informaci těchto značek můžeme získat pomocí NFC zařízení s vlastním zdrojem, nejčastěji smartphonem. Pasivní zařízení z principu nemůžou komunikovat mezi sebou.
- Aktivní NFC zařízení mají vlastní zdroj elektrické energie, dokážou tak komunikat jak s jinými aktivními zařízeními, tak i s pasivními. V případě chytrého mobilního telefonu zdroj představuje baterie sloužící pro napájení všech obvodů.

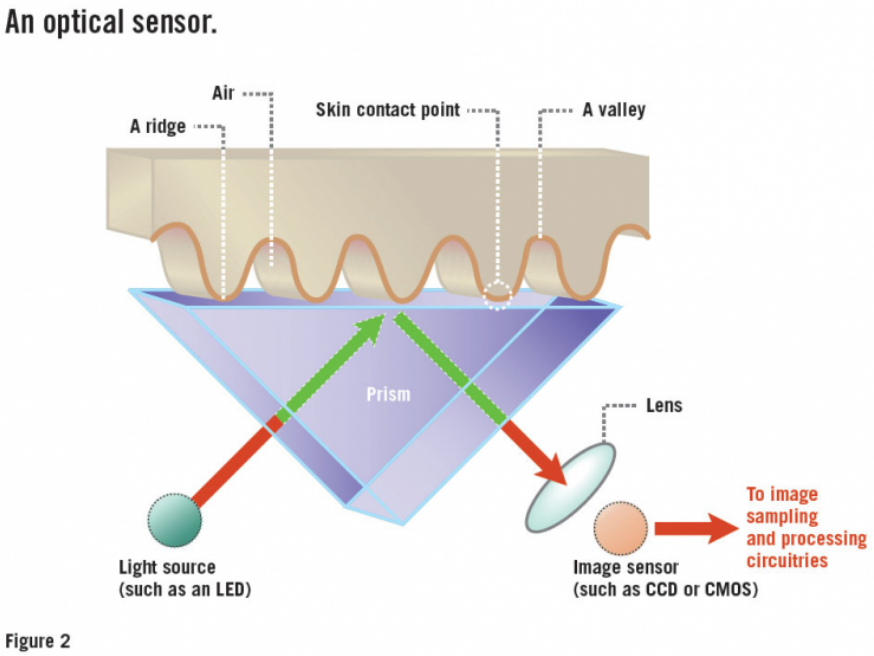
Hlavní rozdíl mezi technologie RFID a NFC je v tom, že zatímco RFID karty jsou výhradně pasivní (aktivních se v EKV příliž nevyužívá) a ke své činnosti potřebují nejprve získat energii pomocí elektromagnetických vln z terminálu, technologie NFC je v rámci identifikace osob založená na aktivním zdroji energie. RFID systémy pro identifikaci osob využívají frekvenci 125 kHz, NFC využívá vysokofrekvenčního systému HF 13,36 MHz stejně jako bezdrátové mikroprocesorové karty.

## 3.5 Identifikace pomocí otisků prstu

Biometrické čtečky otisků prstů využívají k získání obrazu otisků prstů optické, kapacitní nebo ultrazvukové senzory. Všechny metody vytvářejí obraz na základě charakteristických znaků papilárních linií, které nazýváme markanty. Tyto markanty jsou pro každého člověka de-facto identické. V bakalářské práci je biometrická čtečka vybavena optickým senzorem.

### 3.5.1 Optické senzory

Optické metoda snímání papilárních linií patří k nejstarší, ale zároveň dosud nejpoužívanější technologii. Princip činnosti je založený na rozdílném odrazu světla procházejícího optickým hranolem. Využití optického hranolu můžeme vidět na obr. 3.6.




Obr. 3.6: Optický hranol v optických terminálech. Převzato z [11].

Využíváme toho, že odraz světelného toku závisí na tom, zda-li paprsek dopadne na rýhu nebo linii. Od papilární linie se světlo odráží, od rýhy ne. Tyto odrazy světla jsou přenášeny na maticový CCD (Charged-Coupled Device) detektor, který vytvořený obraz digitalizuje a předá k dalšímu zpracování.

# 4 Praktická část semestrální práce

V rámci praktické části semestrální práce je úkolem sestavit výukový model systému elektronické kontroly vstupu EKV. K tomuto účelu byly dodány hardwarové prvky a oblužné softwary, které budou blíže popsány v následujících kapitolách.

## 4.1 Hardwarové komponenty

Byly dodány následující hardwarové komponenty:

- **Ústředna Honeywell NetAXS-123.**
  Základní modul ústředny umožňující ovládat 1 vstup pomocí 1 nebo 2 připojených terminálů, podle toho, zda-li chceme ovládat vstup z jedné nebo z obou stran průchodu. Základní a rozšiřující panely jsou pro komunikaci s připojenými terminály vybaveny komunikačním rozhraním Wiegand v 7 vodičovém provedení, jsou-li připojeny 2 terminály pro 1 dveře, pak v 8 vodičovém provedení. Napájení ústředny lze zajistit připojením vodiče +12 V nebo pomocí technologie Power over Ethernet (PoE). Základní i rozšiřující modul má výstupy, ke kterým jde připojit:
  - 1 terminál pro ovládání 1 dveří nebo 2 terminály pro 1 dveře,
  - odchodové tlačítko,
  - ovládání dveřního zámku a
  - dveřní magnetický kontakt.

  K ústředně se jde připojit správcovským PC pomocí Ethernet kabelu protokolem TCP/IP nebo pomocí USB. Ústředna má dále svorky pro připojení sběrnice RS-485 pro potřeby návazného připojení dalších panelů. V tomto případě lze k bránovému (gateway) ústředně (panelu) připojit až 30 návazných panelů. V takové instalaci má pouze gateway panel vlastní IP adresu.

- **Rozšiřující modul ústředny Honeywell NetAXS-123.**
  Rošiřující modul umožňuje základní panel ústředny rozšířit o řízení dalšího vstupu, tedy připojení až dalších 2 terminálů.

- **Čtečka RFID karet HIDD iClass.**
  RFID terminál s komunikačními rozhraními Wiegand a RS-485 pracující na frekvenci 13,56 MHz. Výstupní velikost Wiegandova slova je 26 bit.

- **4 RFID karty HID iClass GP**.
  Byly dodány radiofrekvenční karty pracující na frekvenci 13,56 MHz.

- **Biometrická čtečka otisků prstů MorphoAccess SIGMA Lite Series.**
  Optická biometrická čtečka pro snímání papilárních linií prstů. Terminál může pracovat zcela samostatně nebo být připojen k ústředně EKV. V případě připojení k ústředně EKV je výstupní formát Wiegand, datovou velikost protokolu lze nastavit v systému MorphoManager. Tento model není vybaven integrovanou čtečkou RFID karet.
  Čtečka je vybavena dvěma rozhraními Wiegand označené jako Wiegand OUT a Wiegand IN a dokáže pracovat jen s jedním z režimů. V režimu Wiegand OUT je možné čtečku připojit k ústředně elektronické kontroly vstupu a pomocí ní ovládat dveřní zámek. V tomto případě jsou využity 3 vodiče Wiegand (datové D0 a D1 a zem GND). V režimu Wiegand IN je možné připojit externí terminál, např. RFID čtečku nebo klávesnici. Takové řešení je možné využít například pokud biometrický terminál není vybaven RFID čtečkou či klávesnicí nebo pokud chceme například umístit tyto terminály na druhou stranu průchodu, který ovládáme. Pro funkci v každém z režimů musejí být využity jiné vodiče, což vychází z principu Wiegandova rozhraní (komunikace je jednosměrná a v každém z režimů probíhá přenos dat opačným směrem).

- **Registrační čtečka otisků prvků Morpho MSO 1300.**
  Čtečka slouží ke snímání referenčních otisků prstů uživatele při registraci uživatele do systémů MorphoManager, který data přenese pomocí IP sítě do biometrického terminálu.

- **PoE přepínač Tenda.**
  Ethernet přepínač vybavený technologií Power over Ethernet, čímž umožňuje napájet připojená zařízení pomocí kabelů UTP. Samozdřejmostí je, že dané zařízení musí tuto technologii podporovat.

- **Odchodové tlačítko.**
  Odchodové tlačítko sloužící k autentizaci při odchodu z vyhrazeného prostoru. Komunikuje s ústřednou pomocí dvojice vodičů.

- **2 elektrické dveřní zámky FAB.**
  Zámky spínané elektrickými impulzy přicházejícími z kontroléru. Doporučené napájecí napětí pro zámek je +12 V stejnosměrné (ss), maximální přípustné napětí údávané výrobcem je +30 V ss. Pro sepnutí/rozepnutí je požadován proud 1 A.

## 4.2 Softwarové komponenty

Byly dodány následující obslužné softwarové programy:

- **Systém MorphoManager.**
  Systém dodáván jako součást produktu MorphoAccess SIGMA Lite Series, který je možné volně stáhnout na stránkách výrobce IDEMA-Morpho. Systém je složen z klinta a serveru. Klientem je počítač, na kterém je instalován software MorphoManager Client, v systému MorphoManager může být instalováno více klientů. Klientská aplikace poskytuje správu přístupových terminálů, registraci úživatelů a tvorbu reportů. Server je počítač, který má nainstalovaný software MorphoManager Server. Server spravuje komunikaci mezi zařízeními Morpho a PC, komunikuje s databází a zpracovává požadavky klientů.

- **Softwarová nadstavba WIN-PAK 4.6 XE.**
  Program WIN-PAK je produkt firmy Honeywell, který umožňuje spravovat více systémů zároveň. Pomocí WIN-PAKu lze do jediného prostředí např. integrovat několik samostatných systémů EKV v budově nebo typově odlišné zabezpečovací systémy. WIN-PAK umožňuje spravovat systémy elektronické kontroly vstupu EKV, kamerové dohledové videosystémy CCTV i systémy elektronické zabezpečovací signalizace EZS. Podobně jako software MorphoManager má i WIN-PAK svou klientskou a serverovou aplikaci.

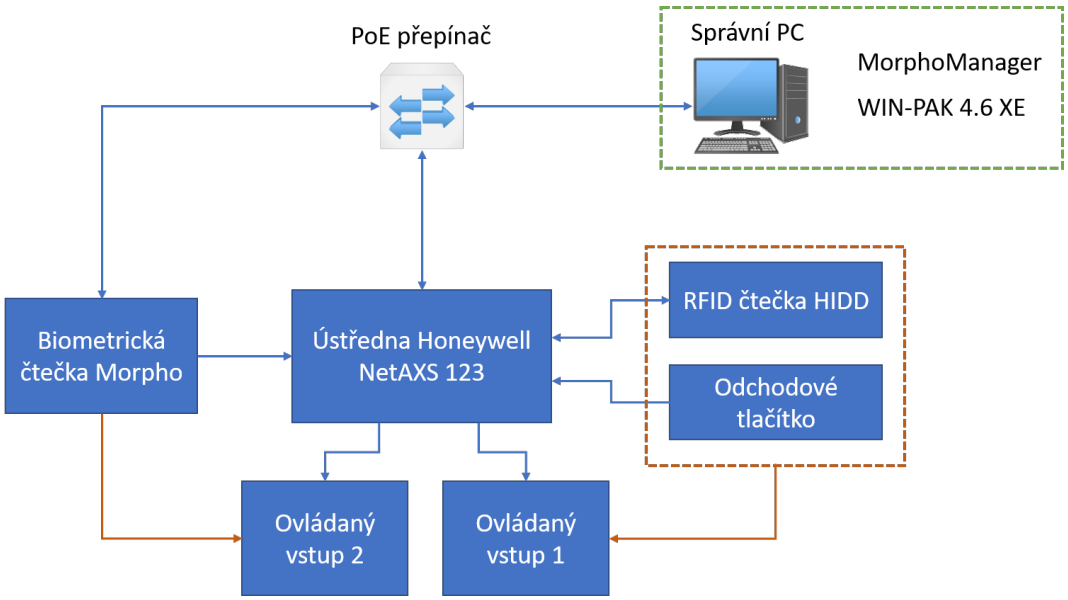
Laboratorní úloha bude běžet ve virtuálním stroji, který bude instalován a spouštěn pomocí technologie VMware.

- **VMware Workstation 15 Player**
  VMware je jedna z technologií umožňující vytvářet jeden nebo více virtualizovaných OS (operačních systémů) v jednom hostitelském OS. Výhodou je možnost virtuální stroje přenášet mezi PC, možnost na jednom PC provozovat více OS nebo jako ochrana při poškození programů. V laboratorní úloze bude virtuální stroj využíván pro rychlou obnovu obslužných programů v případě jejich poruchy pomocí zálohované kopie, která se při vypracování laboratorní úlohy nebude využívat.

## 4.3 Návrh systému EKV

Jelikož byly dodány 2 terminály je ideální navrhovat systém pro řízení průchodu u 2 dveří. Čtečkami by bylo možné ovládat průchod jediných dveří (na každé straně průchodu by byla jedna ze čteček), nebylo by však využito odchodové tlačítko a samotná ústředna by v takovém řešení ani nebyla nutná, protože biometrický termiál Morpho umožňuje připojit externí terminál a mohl by tak v případě 1 dvěřového systémů ústřednu zcela nahradit. Z praktického hlediska je tak systém EKV připraven na budoucí rozšíření.Z důvodu využití potenciálu ústředny je navrhnuto připojení odchodového tlačítka k základnímu panelu spolu s RFID čtečkou HIDD. K rozšiřujícímu panelu pak připojit Wiegand vodiče vedoucí k biometrickému terminálu Morpho. Ke každému z panelů bude připojen jeden zámek. Blokové schema navrhnutého systému EKV lze vidět na obr. 4.1.

Pozn.: Na obr. 4.1 je komunikace Wiegand značená jako obousměrná, ústřena ovládá LED a bzučák RFID čtečky.



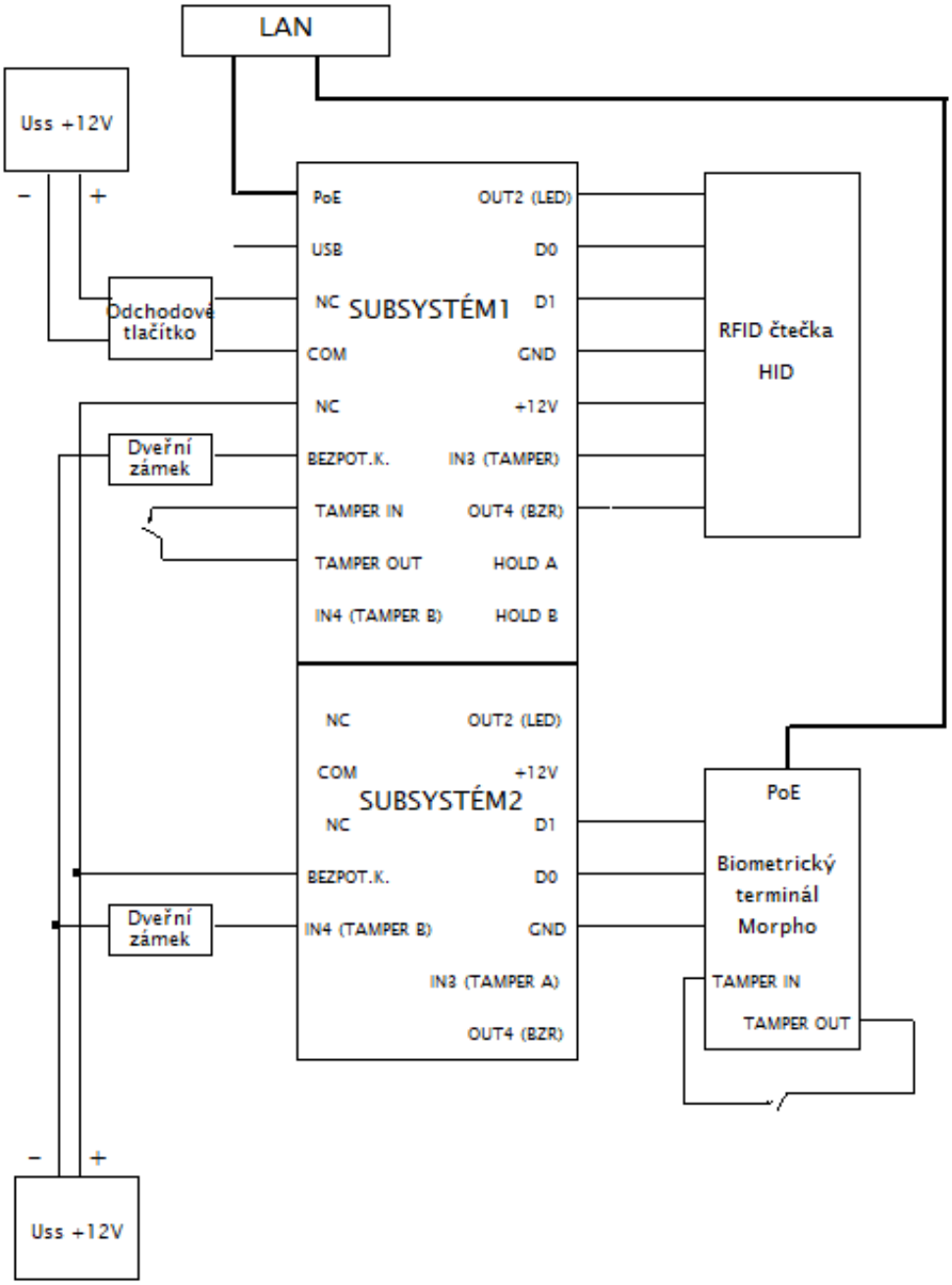

Obr. 4.1: Blokové schema sestavovaného systému EKV.

Systém bude spravován pomocí systémů MorphoManager a WIN-PAK 4.6 XE, oba systémy budou instalovány na správním PC se všemi svými aplikacemi - tedy jak klientskou tak serverovou částí.

## 4.4 Návrh zapojení systému EKV

Hlavní panel a rozšiřující panel ústředny jsou ve schematu zobrazeny ja bloky pod sebou. Hlavní panel je napájen pomocí PoE ethernetového kabelu z PoE přepínače Tenda, rozšiřující panel je napájen z hlavního panelu. K hlavnímu panelu je připojená pomocí sběrnice Wiegand kartová čtečka. Wiegandovo rozhraní má v tomto zapojení 7 vodičů, jsou to datové vodiče D0 a D1, zemní vodič GND, ovládání diody LED, ovládání bzučáku, tamper a napájecí vodič +12 V. Kartová čtečka je tedy zcela napájena pomocí ústředny. Veškerá ostatní připojená zařízení mají vlastní napájení, je to dáno tím, že maximální napájecí napětí technologie PoE je limitované, ústředna na svorkách při napájení PoE dokáže dodat maximálně +12 V (jelikož ústředna má vlastní spotřebu) pro všechna připojená zařízení. To je nedostatečné napětí pro napájení dveřních zámků, každý z nich požaduje +12 V, protože kartová čtečka má určitý odběr, není možné z ústředny napájet ani jeden dveřní zámek. Napájení odchodového tlačítka ústředna NetAXS-123 nepodporuje. Pro napájení celého systému EKV je tedy třeba 3 napajecích zdrojů (pokud nepočítáme napájení PoE přepínače, ten má tedy 4. napájecí zdroj). V řešení je také možnost napájet ústřednu pomocí +12 V, což by umožňovalo napájet dveřní zámky přímo z kontroléru, v celém řešení by se tak ušetřil 1 zdroj elelektrické energie. Tato možnost nebyla preferována, protože systém nebude mít záložní akumulátor a zdroj pro dobíjení akumulátoru není nutný. Pro úsporu počtu napájecích adaptéru bude rozvod pro dveřní zámky rozveden pomocí svorkovnice.

Biometrický terminál Morpho má vlastní tamper vodiče připravené na instalaci k detektoru otevření dveří, pokud není detektor v instalaci použit je nutné vodiče spojit, aby ústředna vyhodnocovala minimální odpor. Čtečka Morpho je k ústředně NetAXS-123 připojena pomocí sběrnice Wiegand v základním 3 vodičovém provedení, tedy jen s datovými vodiči D0, D1 a zemnícím vodičem GND, to je dáno tím, že ověření identity osoby probíhá přímo ve čtečce, která tak přímo ovládá vlastní signalizaci.




Obr. 4.2: Schema zapojení laboratorní úlohy EKV

# 5 Laboratorní úloha Elektronická kontrola vstupu

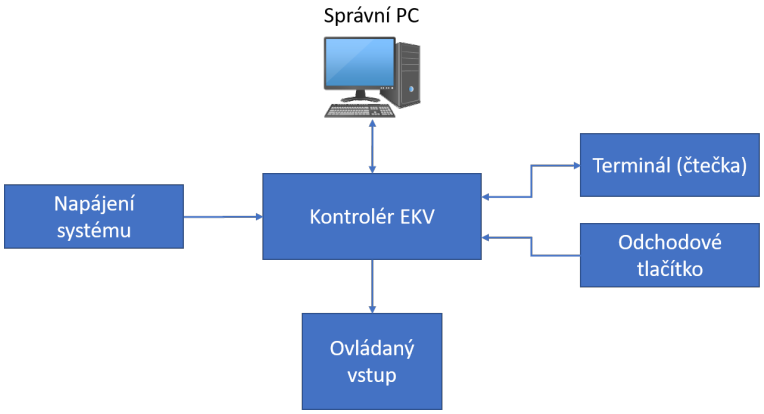
## 5.1 Teoretický úvod

### 5.1.1 Cíl laboratorní úlohy

Úkolem je vytvořit přístupový systém pro ovládání dvou samostatných vstupů. Jeden vstup bude ovládán pomocí radiofrekvenční čtečky HID z jedné strany a odchodového tlačítka z druhé strany dveří. Průchod druhým vstupem bude řízen jednostranně pomocí biometrické čtečky otisků prstů Morpho-Sigma.

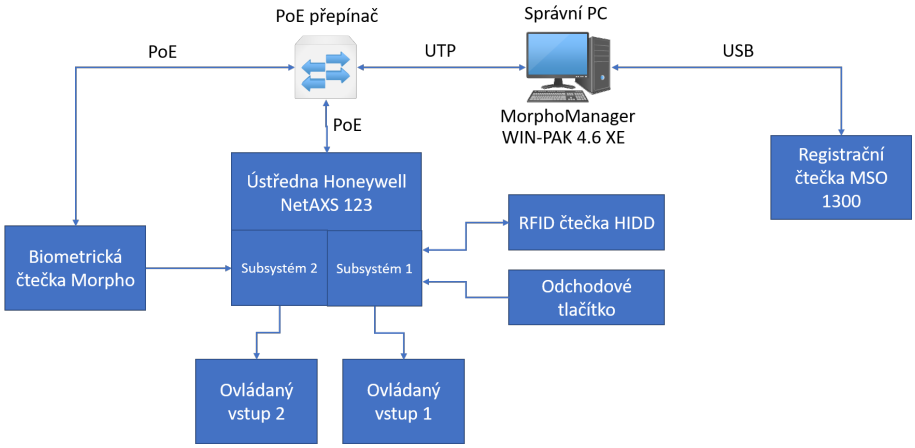
### 5.1.2 Systémy EKV

Systémy elektronické kontroly vstupu (EKV) jsou elektronické systémy, které umožňují řízení přístupu do kontrolované oblasti. Obecné schéma systému EKV můžete vidět na obr. 5.1. K autentizaci uživatele se využívají **terminály**, v úloze jsou využity kartový a biometrický. Terminály (čtečky) identitu poskytnutou uživatelem předají **kontroléru** ve formě Wiegandova slova. Kontrolér neboli ústředna zkontroluje, zda má žadatel právo přístupu do dané oblasti. V kladném případě otevře elektronický zámek a žadatel tak má umožněn průchod. V opačném případě zůstane vstup zablokovaný. Odchodová tlačítka otevřou vstup při jeho zmáčknutí osobou, jsou jednoduchým zařízením, které neprovádí žádnou autenzitaci osoby. Využíváme je tam, kde mají dveři z obou stran kouli.




Obr. 5.1: Obecné schéma systému EKV.

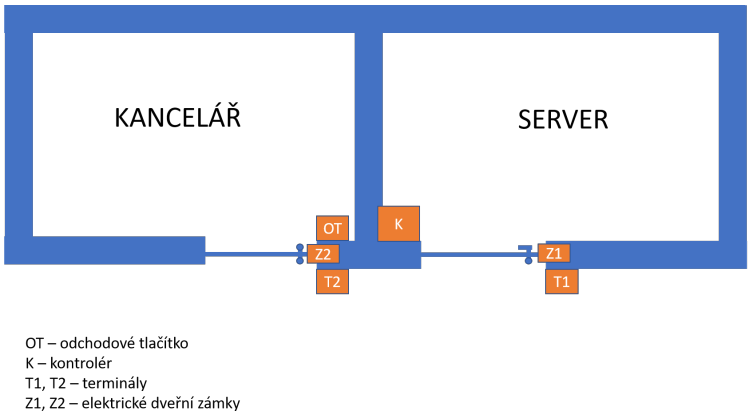
Konkrétní schéma laboratorní úlohy můžete vidět na obr. 5.2 :




Obr. 5.2: Propojení prvků EKV.

Biometrické terminály ve většině případů plní funkci terminálu i kontroléru. Je to z toho důvodu, že autentizace uživatele na základě biometrické veličiny je náročná a typově odlišná pro každý druh biometriky. Z tohoto důvodu autentizaci uživatele provádí samotná biometrická čtečka, která v případě kladného ověření odešle kontroléru Wiegandovo slovo. Toto Wiegandovo slovo musí být zavedeno i v kontroléru, který otevírá dveřní zámek. Autentizace uživatele se tak vlastně provádí dvakrát.

Kontrolér NetAXS-123 využitý v laboratorní úloze dokáže ovládat 2 vstupy pomocí maximálně 4 čteček a připojit 2 odchodová tlačítka. Takže každý vstup může být z každé strany řízen pomocí čtečky. V úloze je jeden vstup řízen pomocí kartové čtečky z jedné strany a odchodového tlačítka z druhé strany a druhý vstup pomocí biometrické čtečky. Možné půdorysné řešení znázorňuje obr. 5.3.




Obr. 5.3: Možné umístění EKV v budově.

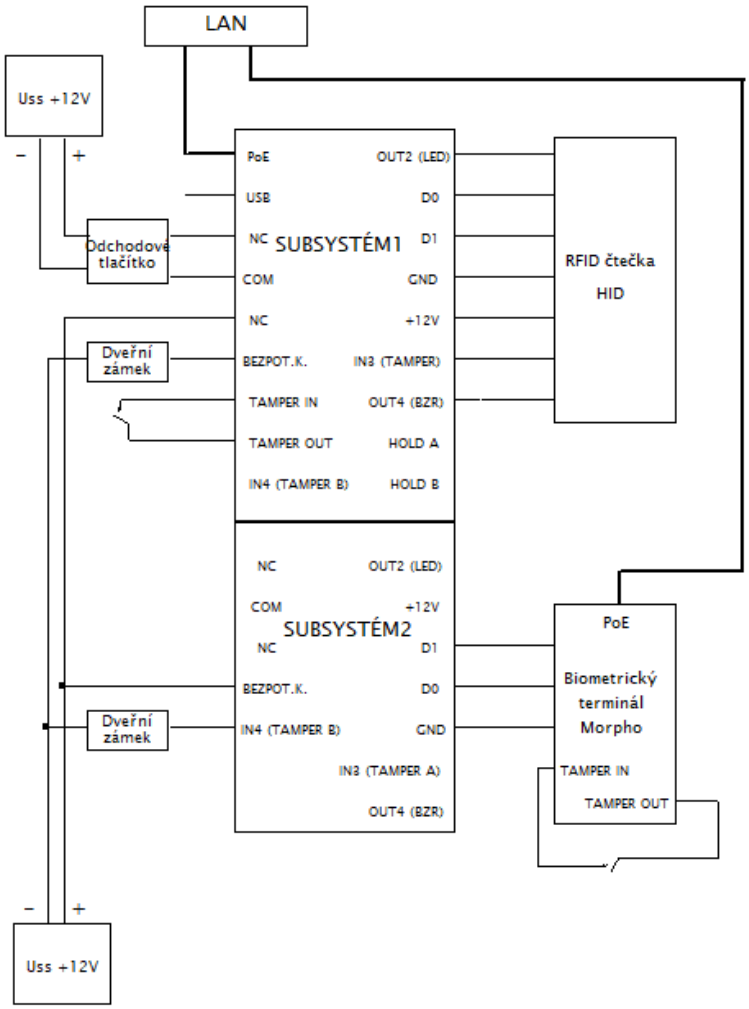
### 5.1.3 Zařízení použité v laboratorní úloze

- Ústředna Honeywell NetAXS-123,
- kartová čtečka HID iClass,
- 4 ks RFID karet,
- biometrická čtečka otisků prstů Morpho-Sigma,
- registrační čtečka otisků prstů MSO-1300,
- odchodové tlačítko,
- 2 elektrické dveřní zámky,
- PoE přepínač Tenda,
- PC s programy WIN-PAK a MorphoManager.

### 5.1.4 Zapojení laboratorní úlohy

Úloha je rozložena na 3 demonstrační panely, kde na 1 panelu je umístěna ústředna EKV, na 2. je umístěná kartová čtečka a odchodové tlačítko ovládající 1. zámek. Na 3. z panelů je biometrický terminál ovládající 2. dveřní zámek. Ústředna a biometrická čtečka jsou připojeny UTP kabely do Power over Ethernet (PoE) přepínače, který zajišťuje napájení a zároveň komunikaci pomocí LAN sítě s obslužnými programy WIN-PAK a MorphoManager.

Kartová čtečka HID a čtečka otisků prstů Morpho jsou ke kontroléru připojeny pomocí sběrnice Wiegand. Wiegandova sběrnice obsahuje vždy minimálně 3 vodiče, systém využívá k signalizaci napětí +5 V na dvou vodičích označovaných D0 a D1. Pomocí odpínání napětí signalizujeme logickou 0 nebo 1, je-li odpojeno napětí na vodiči D0 je vyslána logická 0, přičemž na vodiči D1 zůstává plné napětí 5 V. Je-li odpojeno napětí na vodiči D1, signalizujeme logickou 1. Třetím vodičem je zemnící vodič GND. Výrobci ale sběrnici doplňují o další vodiče, např. pro ovládání LED diody nebo bzučáku - pípače, případně tamper kontakt.




Obr. 5.4: Schéma zapojení laboratorní úlohy.

Ze schématu na obr. 5.4 můžete vidět, že kontrolér NetAXS-123 je logicky rozdělen na dva podsystémy a to hlavní a rozšiřující, kde každý podsystém v našem případě ovládá 1 vstup. Fyzicky je 1. podsystém hlavní (spodní) deska plošného spoje a 2. podsystém je přídavná (horní) deska plošného spoje.

## 5.2 Návod k řešení úlohy

### 5.2.1 Konfigurace čtečky otisků prstů SIGMA

1. Podle blokového schéma úlohy zkontrolujte zapojení úlohy a zapojte veškeré zdroje napájení 230 V. Spusťte virtuální stroj Win7_lab_EKV umístěný na ploše, přihlaště se k uživatelskému účtu student, heslo je student. Nyní jste v roli správce systému EKV a nastavíte jej tak, aby vyhovoval potřebám fiktivní firmy.

2. Nejprve nakonfigurujte čtečku otisků prstů. Spusťte program MorphoManager Client, který naleznete na ploše virtuálního PC a zadejte přihlašovací údaje: - username: administrator - password: password V hlavním okně programu se v horní nabídce přepněte do sekce **Administration** a následně z levé boční nabídky vyberte **Biometric device**. Přidejte nový biometrický terminál pomocí **Add**. Následně vyplňte pole Name (např. ctecka otisku prstu) a u řádku Hardware family vyberte z vysouvací nabídky MA Sigma, MA Sigma Lite. IP adresu zadejte 192.168.1.10 (statická IP adresa biometrické čtečky v LAN sítí laboratorní úlohy) a Biometric device profile vyberte Default. Pomocí Finish dokončete přidávání čtečky. MorphoManager by se měl se čtečkou spojit v lokální LAN síti, synchronizovat se a být ve stavu online, což lze vidět na pravé straně řádku s nově přidanou čtečkou.

3. Nyní přidejte nového uživatele a sejměte jeho otisky prstů. Přejděte do sekce **User Management**, přepnete se opět v horní nabídce programu. Přidejte nového uživatele pomocí Add. Vyplňte libovolně pole First Name; Last Name a Datum narození a pokračujte na další stranu pomocí Next. Vyplňte Employee ID (např. 1) a pokračujte pomocí Next. V tomto okamžiku připojte do USB portu počítače autorizační čtečku otisků prstů MSO 1300 E3, přidávání fotky uživatele neprovádějte a přejděte k dalšímu kroku konfigurace pomocí Next. Nyní jste programem vyzváni k postupnému načtení 3 prstů, jako první vyberte prst na pravé ruce klikem na oranžově blikající část. Je-li registrační čtečka korektně připojena, naskenujte prst 4 krát za sebou dle pokynů programu. Pro kvalitní provedení je třeba na plošku mírně tlačit. Získáte-li v průměru méně než 50 bodů (vaše skeny označeny červenou barvou a varováním) opakujte skenování, případně očistěte snímací plošku. Jsou-li označeny oranžovou barvou jsou vzorky vyhovující ne však ideální. Pro ideální vzorky se snažte dosáhnout více jak 60 bodů, snímky jsou označeny zelenou barvou. Postupně přidejte všechny 3 prsty. Tím je dokončeno přidání nového uživatele.

4. Systém MorphoManager odešle data do čtečky otisků prstů SIGMA, ta by měla přestat blikat zelenou barvu a rozsvítit červené LED diody pod snímací ploškou. Ověřte korektní přidání uživatele přiložením libovolného z naskenovaných prstů, jestliže se čtečka zeleně rozsvítí a zazní akustický signál potvrzení je uživatel nahrán v paměti zařízení a referenční vzory prstů jsou dostačující.

5. Jestliže čtečka po přiložení prstu svítí červěně a neprovádí autentizaci ani jednoho z prstů, opakujte akci přidávání uživatele a snažte se dosáhnout větší přesnosti u vzorků prstů.

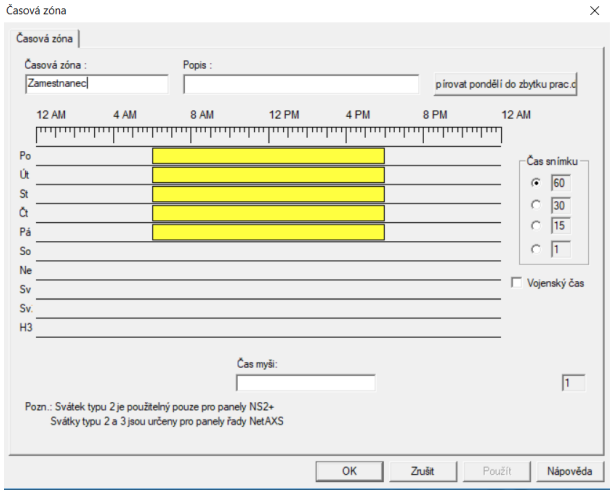
6. Nyní je třeba nastavit vhodný Wiegand profil pro komunikaci s ústřednou EKV, v sekci **Administration** z pravé nabídky přejděme na **Biometric device profile**. 1. list konfigurace přeskočte a přejděte pomocí Next na další list, zde v části nazvané General Settings u Wiegand profile vyberte z vysouvací nabídky: Standart 26 bit. Nyní čtečka otisků prstů posílá pomocí sběrnice Wiegand 5 číselný formát Wiegand do ústředny. Pro ukazováčky je formát stejný, pro prostředníček levé ruky je formát odlišný a pro otevírání dveří jej používat nebudete.

### 5.2.2 Konfigurace ústředny Honeywell NetAXS-123

1. Spusťte program WIN-PAK, který naleznete na ploše pod názvem WIN-PAK User Interface. Zadejte přihlašující údaje: Název: Admin a heslo: Admin2018*.

2. Nejprve je třeba přidat ústřednu Honeywell NetAXS-123 do systému. Z horní nabídky vyberte položku **Konfigurace**, následně **Zařízení** a zvolte **Mapa zařízení**. Klikněte pravým tlačítkem myši na položku Zařízení, zvolte Přidat a následně **Přímé připojení gateway panel NetAXS**. Vyplňtě pole název, např. NetAXS-123_panel (název nesmí obsahovat mezery). V poli Typ vyberte z vysouvací nabídky NetAXS-123-Gateway. Typ komunikace zvolte TCP/IP spojení a následně do nově zobrazeného pole **IP adresa nebo síťový název** zadejte IP adresu 192.168.1.150 (což je IP adresa ústředny). Potvrďte přidání panelu pomocí **Přidat**, následující okno potvrďte a pokračujte v konfiguraci stiskem tlačítka **Další**.

3. Konfiguraci Formátů karet ponechte ve výchozím nastevení a pokračujte dále stiskem **Další**. Nyní je třeba panelu přiřadit s jakými časovými zónami bude pracovat. Časové zóny se používají k časovému omezení přístupu osob do chráněné oblasti.
   Postupně vyberte zóny Vždy a Nikdy z horní tabulky a pomocí šipky je přesuňte do spodní tabulky. Poté vytvořte novou časovou zónu pomocí **Přidat novou čas. zónu** a pojmenujte ji Uklidova_firma, s touto přístupovou úrovní karet budou vstupovat do objektu zaměstnanci externí úklidové firmy. Pomocí tahu myši při současném držení levého tlačítka vyberte u jednotlivých dnů, kdy úklidová firma bude mít přístup do oblasti, čas volte tak, aby jste byly schopni funkčnost otestovat. Potvrďte OK a zařaďte časovou zónu do spodní části tabulky. Stejným postupem vytvořte i časovou zónu Zamestnanec, která bude označovat zaměstnance s povoleným přístupem do budovy od 6:00 do 18:00. V programu WIN-PAK tedy zadejte rozpětí od 6:00 AM do 6:00 PM.




Obr. 5.5: Nastavení časové zóny Zamestnanec.

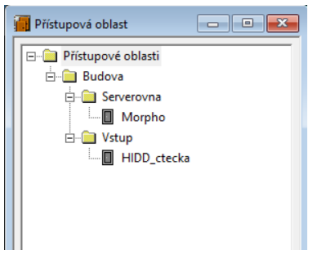
   Pokračujte na další krok stiskem **Další**. Konfiguraci Volby opět ponechte ve výchozím nastavení a pokračujte dále stiskem **Další**.

4. V této části konfigurace nastavíte Vstupy, kde je třeba přiřadit odchodové tlačítko. Dvojklikem na název **1-Žádné ADV** vhodně přejmenujte vstup *, např. Odchodove_tlacitko. Dále musíte nastavit po jak dlouhou dobu po stisku odchodového tlačítka bude sepnutý zámek, tedy jak dlouho po zmáčknutí tlačítka bude možné otevřít dveře. Nastavení provedete v levé spodní části okna, nastavte dobu sepnutí na 5 sekund a přejděte na další krok konfigurace pomocí **Další**.
   * ADV - zkratka ADV v systému WIN-PAK označuje Abstraktní datový vstup.

5. Krok Výstupy ponechte ve výchozím nastavení a pokračujte stiskem **Další** na poslední část konfigurace, kde nastavíte samotné čtečky. Dvojklikem na název čtečky **1a-Žádné ADV** přejmenujte čtečku, např. na HID_ctecka. Podobně jako u odchodového tlačítka je potřeba nastavit po jak dlouhou dobu po přiložení karty bude umožněno otevřít vstup, nastevení provedete kliknutím na blok Výstup 1. V nově otevřeném okně zvolte dobu pulzu 5 sekund.

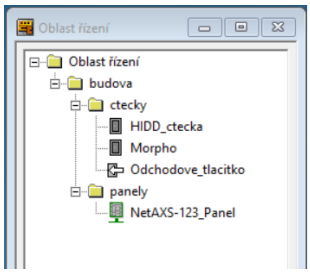
6. Dále podobným postupem přidejte čtečku otisků prstů, nyní aktivujte čtečku pod názvem **2a-Žádné ADV** a vhodně biometrickou čtečku pojmenujte, dobu pulzu pro otevření dveří volte opět 5 sekund. Tímto je hotová konfigurace zařízení. Program vyzve k manuální inicializaci, hlášku potvrďte, inicializace bude provedena později.

7. V následujícím kroku nadefinujete přístupové oblasti, kterými se rozumí rozlišení umístění jednotlivých čteček. Z horní nabídky vyberte **Konfigurace**, dále **Definice** a zvolte **Přístupové oblasti**. V nově otevřeném okně kliknětě pravým tlačítkem myši na název Přístupové oblasti a zvolte přidat větev, pojmenujte ji například Budova. V budově vytvořte další 2 větve, např. Kancelář a Serverovna. Nyní pravým klikem na název Vstup zvolte **Přidat vchody** a vyberte vámi vytvořenou HID_ctecku. Stejným postupem k oblasti Serverovna přidejte biometrickou čtečku. V reálné situaci by Vstup a Serverovna nesměly být příliš vzdálené a být v dosahu ústředny, tj. cca. do 150 metrů.




Obr. 5.6: Nastavení přístupových oblastí.

8. Z horní nabídky opět zvolte **Konfigurace**, dále **Definice** a zvolte **Oblasti řízení**. Zde si opět přidejte novou větev, pojmenujte ji Budova a v ní vytvořte větve Ctecky a Panely. Do větve Ctecky přidejte zařízení pomocí Přidat zařízení, v okně z vysouvací nabídky vyberte Vchod a přidejte obě čtečky pomocí Přidat. Stejně tak do větve Panely přidejte ústřednu NetAXS-123, najdete ji pod položkou Panel. Správná stromová struktura viz. obr. na další straně.

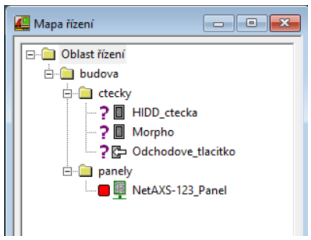



Obr. 5.7: Nastavení oblastí řízení.

9. Poslední části konfigurace ústředny bude nastavení Přístupových úrovní, z horní nabídky zvolte **Karty...** a přejděte na **Přístupové úrovně**. V pravé části by jste měli vidět stejnou stromovou strukturu jakou jste vytvořili v Přístupových oblastech. Pomocí tlačítka **Přidat** vytvořte 3 přístupové úrovně, pojmenujte je Manažer, Zaměstnanec a Úklid. Úrovni Manažer nastavte pravomoc přístupu do všech oblastí, klikněte pravým tlačítkem na Přístupové oblasti v pravé části a zvolte **Nastavit** a následně Nastevení přístupu ke všem vchodům v oblasti a vyberte časovou zónu Vždy. U skupiny Úklid povolte vstup pouze do oblasti Vstup, do serverovny nikoliv a přiřaďte jí časovou zonu Uklidova_firma. Skupině Zaměstnanec povolte přístup do všech oblastí, ale s časovým omezením časové zóny Zaměstnanec. Nyní by u skupiny Manažer a Zaměstnanec měl celý strom mít zelenou barvu a u skupiny Úklid zelenou pouze u oblasti Vstup, u oblasti Serverovna červenou.

10. K ověření funkce systému chybí přidání uživatelů a jejich karet. Z horní nabídky zvolte **Karty...** a přejděte na **Držitelé karet**. V novém okně přejděte na Přidat, vhodně osobu pojmenujte a pokračujte na záložku Karty a opět Přidat. Zadejte číslo jedné z nabídky karet na pracovišti. Do systému WIN-PAK zadejte 5 číselný formát za znaménkem +. Tedy například u karty: 4+09507 42101163121-7 SE, zadáte do systému číslo 09507. Vyberte jednoho z držitele karty (v novém okně je třeba kliknout na Najít) a vyberte Přístupovou úroveň. Tímto postupem vytvořte 4 uživatelů, např. 2 Zaměstnance, 1 zaměstnance Úklidove firmy a 1 Manager.

11. Z horní nabídky programu zvolte **Ovládání** a vyberte **Mapa řízení**. Pokud jste při konfiguraci postupovali správně měly by ve stromu být obsaženy obě čtečky, odchodové tlačítko a ústředna. Pravým tlačítkem klikněte na NetAXS-123_Panel a zvolte Inicializace. Pomocí Zvolit vše zatrhněte všechna pole, potvrďte OK a vyčkejte na dokončení procesu.




Obr. 5.8: Konečný stav.

Po úspěšném připojení program zahlásí **Poruchu napájení**, protože ústředna nemá zálohovaný zdroj napětí. Pokud má ústřena otevřený kryt tak také poruchu **Tamper**. Tyto chyby potvrďte pomocí **Potvrdit**.

12. Otestujte funkčnost RFID čtečky, karty by měly nebo naopak neměly otevírat dveřní zámek podle nastavených časových zón. Pro otestování biometrické čtečky je ještě nutné do programu WIN-PAK přidat generované Wiegandovo slovo jako číslo karty. Přiložte na čtecí plochu jeden z ukazováčků, systém WIN-PAK nahlásí neznámé číslo karty. Číslo, které WIN-PAK ohlásí přidejte do systému jako novou kartu, postupem, který jste prováděli o 2 odstavce výše (viz K ověření systému chybí přídání....), uživateli přiřaďte přístupovou úroveň Manažer.

13. Kompletně nakonfigurovaný systém otestujte a předvěďte vyučujícímu.

## 5.3 Odinstalace systému

1. Nejprve odstraňte záznam v programu MorphoManager. V kartě **User Management** klikněte pravým tlačítkem myši na vytvořenou osobu a zvolte **Delete selected user**. Poté přejděte na kartu **Administration** do skupiny **Biometric device** a pravým klikem myši na vytvořenou čtečku zvolte **Delete**. Biometrická čtečka Morpho by měla začít blikat zelenou barvou a zhasnout snímací LED diody, což značí, že její databáze uživatelů je prázdná.

2. Pokračujte smazáním konfigurace ústředny v programu WIN-PAK. Postupujte přesně podle následujících kroků, jinak vám systém WIN-PAK nebude umožňovat položky smazat, protože jednotlivé položky jsou vzájemně provázané. Přejděte na záložku **Karty...** -> držitelé karet a postupně vymažte jednotlivé osoby pomocí tlačítka **Smazat**. Ve stejné kartě přejděte na **Přístupové úrovně** a pomocí **Smazat** opět smažte všechny přístupové úrovně.
   Přejděte na kartu **Konfigurace**, dále **Definice** a **Oblasti řízení**, pravým klikem na vytvořenou oblast Budova zvolte Odstranit. Ve stejné kartě a záložce přejděte na **Přístupové oblasti** a smažte oblast Budova.

3. Posledním krokem je smazání celé ústředny ze systému, v kartě **Konfigurace** -> **Zařízení** -> **Mapa zařízení** pravým klikem na název ústředny NetAXS-123 vymažte ústřednu pomocí **Odstranit**.

## 5.4 Kontrolní otázky

1. Který prvek systému provádí autentizaci uživatele?
2. Jak se nazývá sběrnice sloužící k propojení čteček s kontroléry a kolik vodičů musí minimálně mít?
3. Který prvek systému provádí autentizaci uživatele u biometrických terminálů?

## 5.5 Možnost další práce

Prostudujte příručky k ústředně Honeywell a biometriké čtečce SIGMA.

# 6 Laboratorní úloha Elektronická kontrola vstupu - informace pro vyučující

## 6.1 Konfigurace ústředny NetAXS-123 pomocí webového rozhraní

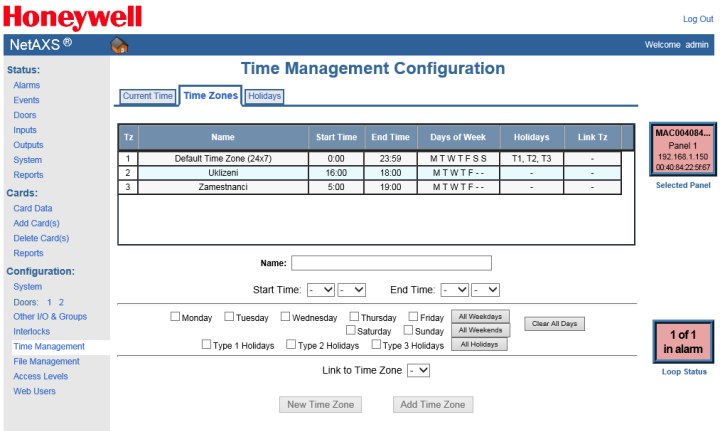
Tento způsob konfigurace je možné použít v případě, že není z jakéhokoliv důvodu možné použít konfiguraci pomocí programu WIN-PAK.

Konfigurace je ideální provádět pomocí prohlížeče Internet Explorer, v jiných prohlížečích webové rozhraní běží zpomaleně nebo nereaguje na příkazy. Na IP adresu ústředny se přihlásíte https://192.168.1.150.

Nejde-li se k ústředně připojit, je možné, že programem WIN-PAK byl webový režim NetAXS-123 zakázán a ústředna si tento stav pamatuje, v tomto případě je třeba ústřednu resetovat pomocí přepínačů DIP. Postup resetování nastavení ústředny naleznete v kapitole: Reset Ústředny NetAXS-123.

Konfigrace probíhá v následujících krocích:

1. Nastevení Režimu komunikace (System configuration). Zvolíme v jakém režimu bude ústředna komunikovat - Webový režim nebo WIN-PAK. V případě konfigurace přes webový prohlížeč nastavíme prioritní webový režim.
2. Nastavení Aktuálního data a času (Current time). Standartní nastavení data a času. Je třeba pro sledování času přístupů jednotlivých karet/osob.
3. Nastavení Časových zón (Time zones). Časové zóny pro jednotlivé skupiny zaměstnanců, přednastavená skupina je Master 24/7, tedy přístup za každých okolností. Možné nastavení skupin můžete vidět na následujícím snímku.




Obr. 6.1: Snímek konfigurace - Nastavení časových zón.

4. Konfigurace Dveří (Doors). Ústředna Honeywell s rozšiřujícím modulem umožňuje ovládat 2 dveře, v konfiguraci označeny jako Dveře 1 a Dveře 2, které z nich právě konfigurujeme si volíte z levé nabídky. Ke každým dveřím lze přidat 2 čtečky, ve webové konfiguraci označené jako Reader A a Reader B.
5. Přidání karet. Karty lze přidávat pomocí Add cards, zadáme číslo karty, jméno držitele karty a zvolíte příslušnou přístupovou úroveň.
6. Sledování stavu systémů a průchodů osob je možné sledovat v záložce Events. Neznáme-li číslo karty, můžeme kartu načíst terminálu a následně její číslo vyčíst v přehledu událostí.

## 6.2 Reset ústředny NetAXS-123

Panel je resetován do továrního nastavení, reset nijak neovlivní nastavenou IP adresu panelu. Pro správné provedení resetu postupujte podle následujících kroků:

1. Poznamenejte si stávající nastavení přepínačů DIP.
2. Při zapnutém napájení panelu přepněte všechny DIP přepínače do polohy VYPNUTO, tj. směrem k vnější hraně panelu.
3. Vypněte napájení a poté jej znovu zapněte.
4. Vyčkejte, než panel naběhne, kontrolka RUN LED (na horní straně desky plošného spoje) by měla rychle blikat. (Pozn. Může se stát, že LED nebliká vůbec i v takovém případě pokračujte, panel se i tak korektně resetuje).
5. Nastavte přepínače DIP zpět do původní polohy.
6. Vypněte napájení a poté jej znovu zapněte.
7. RUN LED by nyní měla blikat normální rychlostí (pozn. než se tak stane trvá několik minut).

Výchozí nastavení DIP ústředny pro potřeby výuky v laboratoři nesouhlasí s výchozím nastavením přepínačů znázorněných v příručce pro konfiguraci NetAXS-123. Je potřeba přepínač číslo 7 nastavit do polohy ON. V této poloze má ústředna statickou adresu 192.168.1.150. V poloze OFF je adresa ústředně přiřazována dynamicky, tato volba v prostředí univerzitní sítě nefungovala.

Po resetu je ústředna standartně nastavena na komunikaci pomocí webového rozhraní a připojení programu WIN-PAK neumožňuje.

## 6.3 Obnovení virtuálního stroje

Obslužné programy běží ve virtuálním stroji technologie VMware Workstation 15 Player pod názvem Win7_lab_EKV. Zástupce, který přímo otevírá virtualizovaný OS je umístěný na ploše. Odkazuje se na soubory umístěné na místním disku D. V případě poruchy je na disku D umístěná záloha pod názvem Win7_lab_EKV_záloha. Obnovíte ji spuštěním souboru Win7_lab_EKV_záloha.wmx.

## 6.4 Import konfigurací WIN-PAK

Do systému WIN-PAK jde importovat konfigurace pomocí programu: WIN-PAK Importovací utilita. Pro možnost importu musí být WIN-PAK registrovaný, tj. nesmí běžet v DEMO režimu. Soubor zálohy s plnou konfigurací pro laboratorní úlohu je uložen na disku D fyzického počítače a také ve virtuálním stroji Win7_lab_EKV pod názvem WIN_PAK_plna.

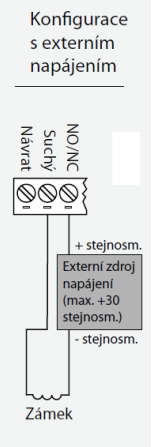
Pro rychlé odstranění konfigurace můžete opět použít Importovací utilitu a nahrát soubor s prázdnou konfigurací. Naleznete opět na disku D fyzického PC nebo virtuálním stroji pod názvem WIN_PAK_prazdna.

# 7 Technická dokumentace

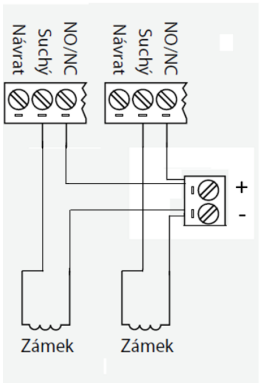
## 7.1 Zapojení labolatorní úlohy

### 7.1.1 Elektrické zámky a rozvod nápajení

Zámky jsou napájené stejnosměrným napětím, v případě nedostatečného napětí pro otevření ústřednou samostatným zdojem posilující ústřednu. Princip můžete vidět na obr. 8.1. Rozvod napájení elektrických zámků v úloze je realizován pomocí svorkovnice. 1 svorka je pro kladný pól a druhá pro záporný. Z rozvodu kladného pólu míří vodiče do ústředny, z rozvodu záporného pólu míří vodiče k zámkům, viz. obr. 8.2.




Obr. 7.1: Princip napájení zámku.



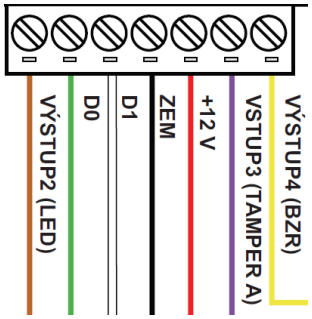

Obr. 7.2: Rozvod napájení v úloze.

### 7.1.2 Čtečka otisků prstů Morpho

Čtečka otisků prstů Morpho je do ústředny připojena pomocí sběrnice Wiegand 3 vodiči. Do ústředny jsou vedeny vodiče D0, D1 a GND, barevné označení odpovídá standartnímu značení Wiegand vodičů podle obr. 8.3. Vodiče jsou na straně čtečky konektorovány společně s elektrických zámkem pomocí 10 pinového konektoru výrobce MOLEX. Vodiče zakončeny dutinkami pro velikost vodiče AWG 22 až 24.

### 7.1.3 Radiofrekvenční čtečka HID

RFID čtečka HID je do ústředny připojena pomocí sběrnice Wiegand 7 vodiči. Na straně čtečky je osazen konektor RJ-45 a dále je mezi ústřednou a čtečkou použit UTP kabel ve kterém je 8. vodič nevyužitý. Zapojení konektoru musí odpovídat připojení sběrnice Wiegand do ústředny podle obr. 8.3. Z obrázku zapojení lze odvodit, jaká barva vodiče Wiegand odpovídá barvě vodiče UTP kabelu.




Obr. 7.3: Zapojení vodičů Wiegand.

### 7.1.4 Odchodové tlačítko

Odchodové tlačítko je do ústředny připojeno pomocí 2 vodičů, na straně tlačítka značeny COM1 a NC, na straně ústředny značeny jako COM a REX. Přičemž NC odpovídá označení REX. Odchodové tlačítko vyžaduje vlastní napájení +12V. Toto napájení není zahrnuto v napájecí svorkovnici pro el. zámky a je odděleno. Důvodem je stálý odběr tlačítka. Integrovaný zemnící kabel tlačítka není v úloze zapojen.


Obr. 7.4: Fotodokumentace zapojení odchodového tlačítka.

## 7.2 Instalace software a nastavení PC

### 7.2.1 Síťové nastavení PC

IP adresu PC je třeba nastavit jako statickou 192.168.1.X s maskou 255.255.255.0. Volba X je libovolná, vyjímkou je volba 10. IP adresa 192.168.1.10 je staticky přiřazena biometrické čtečce Morpho-Sigma. Celý systém byl testován s IP adresou 192.168.1.15.

### 7.2.2 Instalace programu MorphoManager a ovladače MSO 1300

Systém MorphoManager slouží ke správě biometrických zařízení firmy SIGMA-Morpho. Je složen ze serverové a klientské části, ty lze stáhnout z adresy: https://service.morphotrak.com/software-links.html. Na PC se jako první musí instalovat MM Server a až poté MM Client! Při instalaci je nutné produkt online registrovat, pokud se korektně nezaregistruje jsou později některé funkce nefunkční. Prvotní přihlašovací údaje jsou Username: Administrator a heslo: password.

Při prvotním připojení USB čtečky MSO 1300 E3 OS MS Windows stáhne ovladač, tento ovladač odinstalujte (jde o defaultní ovladač pro USB zařízení z nabídky Microsoft). V nastavení OS otevřte **Aplikace a funkce** a vyhledejte Morpho USB driver. Poté stáhněte správný MSO driver ze stránek https://service.morphotrak.com/software-links.html. Stažený ZIP soubor dekomprimujte, následně podle verze operačního systému (x64 nebo x84) vyberte archiv a ZIP soubor **data1** dekomprimujte.

Následně otevřete **Správce zařízení** systému MS Windows a vyhledejte zařízení MSO 1300 E3, pravděpodobně se bude nacházet ve skupině Řadiče USB. Pravým klikem vyberte Aktualizovat ovladač a následně zvolte Vyhledat ovladač v počítači. Vyberte dekomprimovanou složku Data1. Systém provede instalaci a poté lze autorizační čtečku využívat v programu MorphoManager.

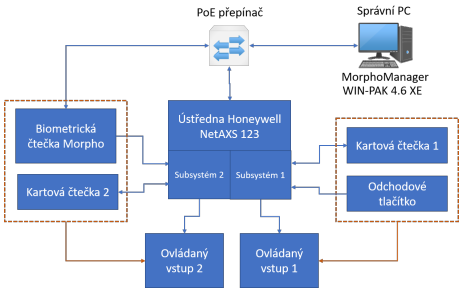
### 7.2.3 Instalace programu WIN-PAK 4.6

Systém WIN-PAK je dodáván na instalačních DVD. Úvodní obrazovka nabídne možnosti: Instalovat software, Registrace programu a Dokumentace. Není nutné WIN-PAK registrovat, program pracuje v DEMO režimu, který je pro potřeby laboratorní úlohy dostačující. Po vložení instlačního DVD spusťně instalaci a po vyzvání zadejte CD klíč. Zvolte uplnou instalaci, kde je server i klient instalován na jediném PC. Při instalaci SQL databáze budete vyzváni k vytvoření účtu, tento účet posléze **neslouží** jako přihlašovací údaj do systému WIN-PAK. Po dokončení instalace se přihlaste pomocí jména: admin, heslo nevyplňujte a zvolte nové přihlašovací údaje.

## 7.3 Možnosti budoucího rozšíření systému

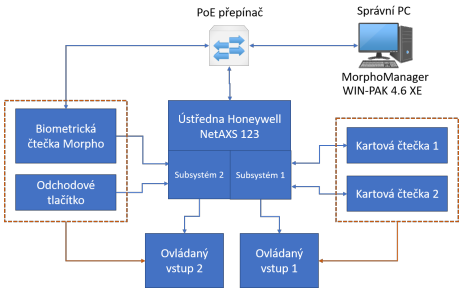
Systém je možné doplnit o další kartový nebo biometrický terminál a to buď bez jakéhokoliv zásahu do současného rozvržení laboratorní úlohy anebo se změnou rozvržení.

- Nejjednodušší možností je doplnění vstupu s biometrickou čtečkou o další kartový terminál z druhé strany vstupu. Vodiče Wiegand budou zapojeny do 2. subsystému kontroléru (do horní desky plošného spoje). Wiegand v zapojení 2 čteček pro 1 vstup využívá 8 vodičů, 8. vodič je tzv. čekací linka. Biometrický terminál Morpho nemá vodič čekací linky, výrobce zřejmě neočekával oboustranného řízení přístupu pomocí kontroléru. Z tohoto důvodu by čekací linky využívala jen kartová čtečka.




Obr. 7.5: 1. možnost rozšíření laboratorního systému EKV.

- Druhou možností, která vyžaduje změnu zapojení systému EKV je přepojení odchodového tlačítka do subsystému 2. Tzn. vstup, kde je autentizace prováděna jen čtečkou z jedné strany vstupu by bylo přidáno odchodové tlačítko na druhou stranu vstupu. Novou kartovou čtečku by jsme připojili do subsystému 1 k současně připojené kartové čtečce HID. Vstup by byl z každé strany řízen kartovou čtečkou. Výhodou je eliminace problému s čekací linkou, protože kartové čtečky vodič čekací linky standartně obsahují.




Obr. 7.6: 2. možnost rozšíření laboratorního systému EKV.

# 8 Závěr

V teoretické části bakalářské práce bylo úkolem obecně popsat problematiku Elektronické kontroly vstupu. Byly popsány výhody nasazování těchto systémů, jejich architektura, možnosti budoucího vývoje v rámci IP sítě a napájení pomocí technologie Power over Ethernet. Dále jsem se zabýval metodami autentizace a samotným popisem autentizačních neboli identifikačních technologií. Největší prostor jsem věnoval radiofrekvenčním technologiím, které jsou v praxi nejvyužívanější, zmíněny byly i starší technologie jako Wiegandovy a magnetické karty a nastíněna byla technologie NFC. Z biometrických technologií byla popsána optická metoda snímání otisků prstů, právě tato technologie byla využita v rámci praktické části bakalářské práce.

V praktické části bylo úkolem na základě dodaných komponent navrhnout výukový systém EKV, zpracovat detailní schéma jeho zapojení, popsání jeho možností a následně tento systém sestavit jako demostrační pro potřeby laboratorní úlohy. Dále vytvořit text návodu laboratorní úlohy pro studenty, doplňující informace pro vyučující a zpracovat technickou dokumentaci systému.

Na základě dodaných komponent jsem navrhnul systém umožňující realizovat kontrolu vstupu u 2 vstupů, přičemž průchod prvním vstupem je řízen z jedné strany pomocí biometrické čtečky MorphoAccess SIGMA Lite a druhý vstup je řízen oboustranně pomocí RFID čtečky z jedné strany a odchodovým tlačítkem ze strany druhé. Dle návrhu jsem systém realizoval na 3 demostrační panely, které jsou vzájemně rozpojitelné.

Bakalářskou práci hodnotím jako velmi praktickou, seznámil jsem se velmi dobře po teoretické i praktické stránce se systémy Elektronické kontroly vstupu a vlastnostmi zařízení používané v této oblasti.

# Literatura


[1] VUT v Brně: *Úprava, odevzdávání a zveřejňování vysokoškolských kvalifikačních prací na VUT v Brně* [online]. Směrnice rektora č. 2/2009. Brno: 2009, poslední aktualizace 24. 3. 2009 [cit. 23. 10. 2015]. Dostupné z URL: <https://www.vutbr.cz/uredni-deska/vnitrni-predpisy-a-dokumenty/smernice-rektora-f34920/>.

[2] *ČSN ISO 7144 (010161) Dokumentace – Formální úprava disertací a podobných dokumentů.* 24 stran. Praha: Český normalizační institut, 1997.

[3] BIERNÁTOVÁ, O., SKŮPA, J.: *Bibliografické odkazy a citace dokumentů dle ČSN ISO 690 (01 0197) platné od 1. dubna 2011* [online]. 2011, poslední aktualizace 2. 9. 2011 [cit. 19. 10. 2011]. Dostupné z URL: <http://www.citace.com/CSN-ISO-690.pdf>

[4] *Personalizace*. Tanatar [online]. Praha 11 Chodov: Tanatar [cit. 2018-10-31]. Dostupné z URL: <http://idstandard.cz/>.

[5] *How does RFID tag technology works*. ScienceProg [online]. 2007 [cit. 2018-12-08]. Dostupné z URL: <https://scienceprog.com/how-does-rfid-tag-technology-works/>.

[6] Burda, K. *Základy elektronických zabezpečovacích systémů*. CERM, Brno 2018.

[7] *Power over Ethernet*. Power over Ethernet [online]. 2018 [cit. 2018-12-08]. Dostupné z URL: <https://en.wikipedia.org/wiki/Power_over_Ethernet/>.

[8] MRÁZEK, Oldřich. *Princip činnosti Power Over Ethernet* [online]. 2004 [cit. 2018-12-08]. Dostupné z URL: <https://vyvoj.hw.cz/produkty/ethernet/princip-cinnosti-power-over-ethernet.html/>.

[9] Honeywell. *NetAXS-123: Access Control Unit Installation Guide, 800-05779V2*. 2013 [cit. 2018-12-08].

[10] SAFRAN-Morpho. *MorphoManager: User Manual*.

[11] *Čtečky otisku prstů pod drobnohledem – jak fungují?*. Mobilizujeme [online]. 2018 [cit. 19.05.2019]. Dostupné z URL: <https://mobilizujeme.cz/clanky/ctecky-otisku-prstu-pod-drobnohledem-jak-funguji>.